CommandCenter®
Secure Gateway



CC-SG
管理员指南
版本 3.1

CCA-0D-CHS
2007 年 1 月
255-80-5140-00

此页专门留白。

FCC 信息

本设备已经测试并符合 FCC 规则第 15 部分对有关 A 类数码装置的限制要求。这些限制的设计为商业安装中的有害干扰提供合理保护。本设备产生、使用并辐射无线频率能量，如果不按照说明进行安装和使用，则可能对无线通信产生有害干扰。在居民环境中运行本设备可能产生有害干扰。

日本认可

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

由于事故、灾害、误用、滥用、对产品进行非 Raritan 的修改或者其它在 Raritan 合理控制范围之外的事件，或并非在正常工作条件下而出现的产品损坏，Raritan 概不承担责任。

CE c UL US LISTED 1F61 I.T.E.

在南美或北美地区寻求协助，请联系 Raritan 技术支持团队：
电话 (732) 764-8886，传真 (732) 764-8887，电子邮件 **tech@raritan.com**
技术支持时间：周一至周五，早 8 点至晚 8 点（东部时间）。

在世界范围内寻求协助，请查阅本指南的最后一页有关区域 Raritan 办事处的联系信息。

安全指南

要避免潜在的致命电击危险以及对 Raritan 设备可能的损坏：

- 不要在任何产品配置上使用两芯电源线。
- 在计算机和监视器处测试交流电源插座，查看极性和接地是否正常。
- 在计算机以及监视器上仅使用接地的电源插座。使用备用 UPS 时，请断开计算机、监视器和设备的电源。

机架安装安全指南

在需要机架安装的 Raritan 产品中，请遵照以下注意事项：

- 封闭机架环境中的工作温度可以高于室内温度，但不得超过该设备的最大额定环境温度。请参阅附录 A：规格（G1、V1 和 E1）。
- 保证机架环境中充分的空气流动。
- 在机架中小心安装设备，以免产生不均匀机械负荷。
- 小心将设备连接到供电电路，避免产生电路过载。
- 要将设备正确接地至分支电路，尤其是电源连接，如配电盘（而非直接连接）。

目录

图目录

第 1 章：简介

祝贺您购买 CommandCenter Secure Gateway (CC-SG)，这是 Raritan 用于管理各种 UNIX 服务器、防火墙、路由器、载荷均衡器、电源管理设备和 Windows 服务器而提供的方便而安全的方法。

CC-SG 使用一套串行和 KVM 设备提供集中的操作和管理。其设计可在各种环境内工作，从高密度数据中心、服务提供商环境到处理大型远程办公室的公司环境。

CC-SG 与 Raritan 的 Dominion 或 IP-Reach 端口级管理设备联合使用时，可改善和简化目标设备（称为“节点”）的管理，通过连接 IP 网络并且提供被管网络内所有目标设备的串行控制台和 KVM 端口，方便数据中心设备的管理。

前期准备

在按照本文的步骤配置 CC-SG 之前，请参阅 Raritan 的《数字解决方案部署指南》全面了解如何部署受 CC-SG 管理的 Raritan 设备。

目标读者

本文适于通常拥有所有可用权限的管理员。请参阅**附录 C：用户组权限**。非管理员用户通常具有较少的权限，例如仅被授予“节点访问”权限。这些用户应参阅 Raritan 的《CommandCenter Secure Gateway 用户指南》了解详情

术语/缩略语

本文档中使用以下术语和缩略语：

- **访问客户端**——普通用户访问受到 CC-SG 管理的节点时所用的基于 HTML 的客户端。访问客户端不允许使用管理功能。
- **关联**——类别、类别元素与端口或设备（或端口及设备）之间的一种关系。例如，如果想要将“Location”类别与设备关联，则在 CC-SG 中添加设备和端口之前先创建关联。
- **类别**——包含一系列值或元素的变量。比如类别“Location”可含有“New York City”、“Philadelphia”或“数据中心 1”等元素。将设备和端口添加到 CC-SG 时，将会把此信息与其关联。更简单的方法是在向类别中添加设备和端口之前，先正确设置关联。比如类别“OS 类型”可含有“Windows®”、“Unix®”或“Linux®”等元素。
- **CIM**（Computer Interface Module，计算机接口模块）——用于连接目标服务器和 Raritan 设备的硬件。每个目标需要一个 CIM，但 Dominion KX101 除外，因为它与一个目标直接连接，不需要 CIM。目标服务器应打开并连接到 CIM，CIM 应连接到 Raritan 设备，然后才能在 CC-SG 中添加设备和配置端口。否则，空白的 CIM 名称将会覆盖 CC-SG 端口名称。服务器连接 CIM 后需要重新启动。
- **CommandCenter NOC** (CC NOC) ——一种网络监视设备，用于审计和监视 CC-SG 所管理的服务器、设备和 Raritan 设备的状态。
- 设备组——某个用户可以访问的已定义的设备组。设备组用于创建策略时控制对组内设备的访问。
- **设备**——受到 CC-SG 管理的 Raritan 设备，例如 Dominion KX116、Dominion SX48、Dominion KSX440、IP-Reach、Paragon II System Controller、Paragon II UMT832 with USTIP 等。这些设备控制与其相连的目标服务器和系统。
- **Director Client**—CC-SG 的一个基于 Java 的客户端，普通用户和管理员均可使用。它只唯一允许进行管理的客户端。
- **元素**——类别的值。例如，“New York City”元素属于“Location”类别。或者，“Windows”元素属于“OS 类型”类别。

- **幻影端口**——在管理 Paragon 设备时，当 CIM 或目标设备从系统中删除或关闭（手动或意外关闭）时，即会出现幻影端口。详情参见 Raritan 的《Paragon II 用户手册》。
- **主机名**——如果启用 DNS 服务器支持，则可使用主机名。详情参阅**第 12 章：高级管理**中的“网络配置”。主机名及其完全限定的域名（FQDN = 主机名 + 后缀）不能超过 257 个字符。可包含任意多个部分，只要用“.”隔开即可。每个部分最长 63 个字符，第一个字符必须为字母。其余字符可以是字母、数字或“-”（破折号或减号）。每个部分的最后一个字符不能是“-”。虽然系统保留字母输入系统时的大小写，但 FQDN 在使用时不分大小写。
- **iLO/RILOE**——可被 CC-SG 管理的惠普 Integrated Lights Out/Remote Insight Lights Out 服务器。iLO/RILOE 设备的目标可直接打开电源、关闭电源或循环电源。iLO/RILOE 设备不能被 CC-SG 发现，而是要手动添加为节点。
- **带内访问**——通过 TCP/IP 网络对网络中的目标进行纠正或故障排除。KVM 和串行设备可通过以下带内应用程序进行访问：**RemoteDesktop Viewer**、**SSH Client**、**RSA Client**、**NC Viewer**。
- **IPMI 服务器**（智能平台管理接口）——可由 CC-SG 进行控制的服务器。IPMI 可被自动发现，也可以手动添加。
- **带外访问**——使用 Raritan Remote Console (RRC)、Raritan Console (RC) 或多平台客户端 (MPC) 等应用程序来对网络中的 KVM 或串行被管节点进行纠正或故障排除。
- **策略**——定义某个用户组可以访问的权限、访问类型以及访问的端口和设备。策略应用到用户组，有几个控制参数来决定控制级别，例如访问日期和时间。
- **节点**——CC-SG 用户可访问的目标系统，例如服务器、桌面 PC 或其它组网设备。
- **接口**——接口是可以访问节点的途径，不论通过带外解决方案（如 Dominion KX101 连接）或通过带内解决方案（如 VNC 服务器）。
- **节点组**——某个用户可以访问的已定义的节点组。节点组用于创建策略时控制对组内节点的访问。
- **端口**——Raritan 设备和节点之间的连接点。端口仅存在于 Raritan 设备上，标识从该设备到某个节点的路径。
- **SASL**——（Simple Authentication and Security Layer，简单认证和安全层）。一种向基于连接的协议添加认证支持的方法。
- **SSH**——客户端（例如 Putty 或 OpenSSH），向 CC-SG 提供一种命令行界面。仅通过 SSH 为管理设备和 CC-SG 本身提供 CC-SG 命令的子集。详情参见**第 12 章：高级管理**。
- **用户组**——共享同一个访问和权限级别的用户集合。例如，默认用户组“系统管理员”具有对所有配置任务和目标节点的完全访问权。

第 2 章：访问 CC-SG

为 CC-SG 配置 IP 地址以后，CC-SG 设备即可放置到其最终目标位置。完成设备运行所需的所有必要硬件连接。

您可以多种方式访问 CC-SG，本章将分别予以介绍：

- **浏览器**：CC-SG 支持很多种 Web 浏览器。（有关所支持的浏览器和平台完整列表，请参照 **http://www.raritan.com/support** 上的“兼容性矩阵”。在“支持”页面上，单击“固件升级”，然后单击 **CommandCenter Secure Gateway**）。
- **胖客户端**：可在客户端计算机上安装一个 Java Web Start 胖客户端。胖客户端功能非常类似基于浏览器的客户端。
- **SSH**：通过串口连接的远程设备可使用 SSH 进行访问。详情参阅第 12 章：高级管理。
- **诊断控制台**：仅提供紧急维修和诊断，不能代替基于浏览器的 GUI 来配置和操作 CC-SG。详情参阅第 12 章：高级管理。

注：访问 CC-SG 时，用户可使用浏览器、单机客户端和 SSH 同时连接。

基于浏览器访问

1. 使用一个支持的 Internet 浏览器，键入以下 URL：**https://<IP_address>/admin**，其中 <IP_address> 为 CC-SG 的 IP 地址。例如 **https://10.20.3.30/admin**。
2. 出现安全警告窗口时，单击“是”继续。
3. 如果机器上使用不受支持的 Java Runtime Environment 版本，则将会出现警告。从弹出的窗口中，选择是否从 CC-SG 服务器（如果可用）下载正确的 JRE 版本，从 Sun Microsystems 网站下载，或者继续使用不正确的版本，然后单击“确定”。出现“登录”窗口。



图 1 登录窗口

4. 如果启用“有限服务协议”，请阅读协议文本，然后选取“我理解并接受有限服务协议”复选框。
5. 键入“用户名”和“密码”，然后单击“登录”。

胖客户端访问

CC-SG 胖客户端通过启用 Java Web Start 应用程序连接 CC-SG，而不是通过 Web 浏览器运行 Applet 进行连接。使用胖客户端代替浏览器的优点是，客户端的速度和效率要胜过浏览器。

安装胖客户端

1. 要从 CC-SG 下载胖客户端，请启动一个 Web 浏览器，然后键入以下 URL：**http(s)://<IP_address>/install**，其中 <IP_address> 为 CC-SG 的 IP 地址。
2. 如果出现安全警告消息，单击“开始”继续下载。
3. 如果客户端计算机正在运行 Java 版本 1.4，则出现一个“桌面集成”窗口。如果想要 Java 在桌面上为胖客户端添加一个快捷图标，单击“是”。
4. 下载完成后，出现一个新窗口，其中可指定 CC-SG IP 地址。



图 2 胖客户端 IP 地址指定窗口

5. 在“待连接 IP”字段中键入要访问的 CC-SG 设备的 IP 地址。连接以后，即可从“待连接 IP”下拉列表中使用此地址。IP 地址存储在一个属性文件中，该文件保存在桌面上。
6. 如果 CC-SG 配置为安全浏览器连接，则必须选中“安全套接字层 (SSL)”复选框。如果 CC-SG 未配置为安全浏览器连接，则必须清除“安全套接字层 (SSL)”复选框。此设置必须正确，否则胖客户端将无法连接 CC-SG。
   - **要检查 CC-SG 中的设置：**从“管理”菜单中，单击“安全”。在“常规”选项卡内，查看“浏览器连接协议”字段。如果选择了“HTTPS/SSL”选项，则必须在胖客户端的 IP 地址指定窗口中选中“安全套接字层 (SSL)”复选框。如果选择了“HTTP”选项，则必须在胖客户端的 IP 地址指定窗口中清除“安全套接字层 (SSL)”复选框。
7. 单击“开始”。
   - 如果机器上使用不受支持的 Java Runtime Environment 版本，则会出现警告消息。请按照提示下载一个支持的 Java 版本，或者继续使用当前安装的版本。
8. 出现登录屏幕，胖客户端的外观和操作类似基于浏览器的 Java 客户端。如果启用“有限服务协议”，请阅读协议文本，然后选取“我理解并接受有限服务协议”复选框。
9. 在相应的字段中键入“用户名”和“密码”，然后单击“登录”继续。

使用胖客户端

胖客户端安装以后，可通过两种不同的方式从客户端计算机进行访问。这取决与当前使用的 Java 版本。

- **Java 1.4.x**

如果客户端计算机上正运行 **Java 版本 1.4.x**，并且安装胖客户端时在“桌面集成”窗口中单击“是”，则可双击桌面上的快捷图标启动胖客户端并访问 CC-SG。如果没有快捷图标，可随时进行创建：在客户端计算机上搜索 **AMcc.jnlp**，然后创建该文件的快捷方式。

- **Java 1.5**

如果客户端计算机正在运行 Java 版本 1.5，则可以：

a 从 Java 控制面板的“Java 应用程序高速缓存查看器”中启动胖客户端。

b. 使用 Java 控制面板的“Java 应用程序高速缓存查看器”在桌面上为胖客户端安装一个快捷图标。

CC-SG 窗口组件

有效登录后，出现 CC-SG 应用程序窗口。

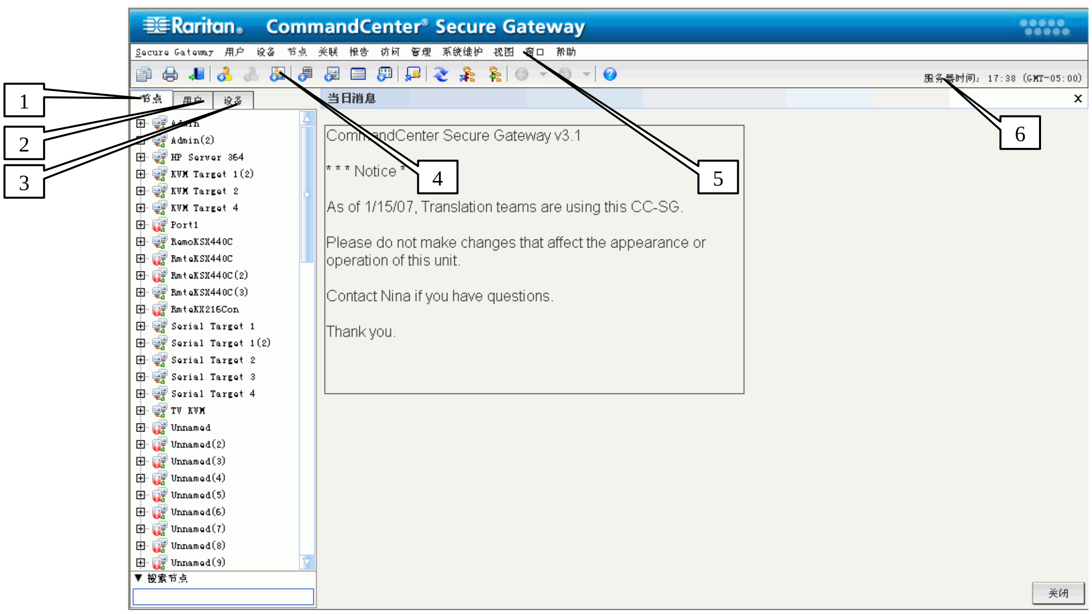


图 3 CC-SG 窗口组件

1. **节点选项卡：**单击“节点”选项卡在树形视图中显示所有已知目标节点。单击一个节点即可查看节点配置文件。接口在其父节点下分组。单击 + 和 - 符号即展开和收缩树。右键单击一个接口并选择“连接”即连接到该接口。可按“节点名称”（字母顺序）或“节点状态”（可用、忙碌、不可用）对节点进行排序。右键单击树形视图，选择“节点排序选项”，然后选择“按节点名称”或“按节点状态”。
2. **用户选项卡：**单击“用户”选项卡，即可在树形视图内显示所有已注册的用户和组。单击 + 和 - 符号即展开和收缩树。
3. **设备选项卡：**单击“设备”选项卡，即可在树形视图内显示所有已知的 Raritan 设备。不同的设备类型有不同的图标。端口在其父设备下分组。单击 + 和 - 符号即展开和收缩树。单击一个端口即可查看端口配置文件。右键单击端口并选择“连接”即连接到该端口。可按“端口名称”（字母顺序）或“端口状态”（可用、忙碌、不可用）对端口进行排序。右键单击树形视图，选择“端口排序选项”，然后选择“按节点名称”或“按节点状态”。

4. **快速命令工具栏**：此工具栏提供一些用于执行常见命令快捷按钮。
5. **操作和配置菜单栏**：这些菜单含有操作和配置 CC-SG 所用的命令。可在“节点”、“用户”和“设备”选择选项卡内右键单击图标来访问其中的部分命令。所能看到的菜单和菜单项取决于用户访问权限。
6. **服务器时间**：在“配置管理器”中 CC-SG 上配置的当前时间以及时区。在“任务管理器”中计划任务时将用到此时间。详情参阅**第 12 章：高级管理**中的“任务管理”。此时间与客户端上所用的时间可能不同。

检查 IP 地址、固件版本和应用程序版本

登录后应确认 IP 地址、设置 CC-SG 服务器时间、检查所安装的固件和应用程序版本。可能需要升级固件和应用程序。

确认 IP 地址

1. 从“管理”菜单中，单击“配置”打开“配置管理器”屏幕。
2. 单击“网络设置”选项卡。

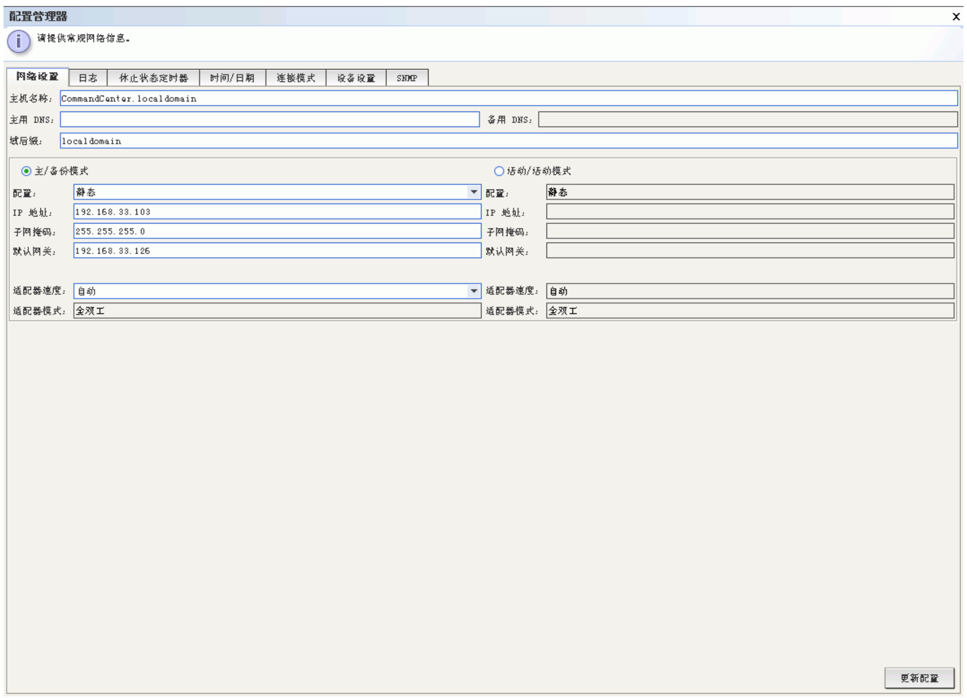


图 4 确认 IP 地址

3. 检查网络设置是否正确并进行必要的更改。
4. 单击“更新配置”提交更改。
5. 在出现的确认窗口中单击“确定”确认设置、注销并重新启动 CC-SG。
6. 使用新的 IP 地址访问 CC-SG。

设置 CC-SG 服务器时间

1. 登录 CC-SG。
2. 从“管理”菜单中，单击“配置”打开“配置管理器”屏幕。
3. 单击“时间/日期”选项卡。

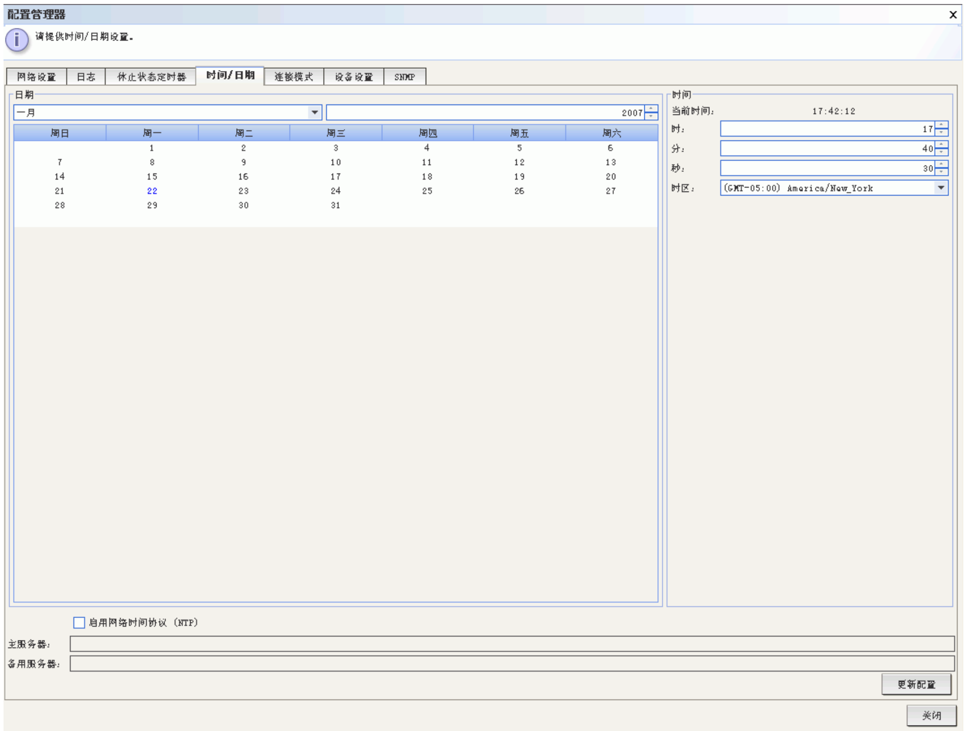


图 5 时间/日期配置

4. 从“管理”菜单中，单击“配置”打开“配置管理器”屏幕。
5. 单击“时间/日期”选项卡。
   a. **手动设置日期和时间：日期**——单击下拉箭头选择“月”，使用上/下箭头选择“年”，然后在日历区域选择“天”。**时间**——使用上/下箭头设定“时”、“分”和“秒”，然后单击“时区”下拉箭头选择操作 CC-SG 所在的时区。
   b. **要通过 NTP 设置日期和时间**：选中窗口底部的“启用网络时间协议”复选框，在相应的字段中键入“主用 NTP 服务器”和“备用 NTP 服务器”的 IP 地址。

注：网络时间协议 (NTP) 是将所连计算机的日期和时间数据与基准 NTP 服务器进行同步的协议。CC-SG 配置 NTP 后，即可与公共可用的 NTP 基准服务器同步时钟时间，并维护正确和一致的时间。

6. 单击“更新配置”将时间和日期更改应用到 CC-SG。
7. 单击“刷新”即在“当前时间”字段中重新载入新的服务器时间。
8. 从“维护”菜单中，单击“重新启动”即重启 CC-SG。

检查和升级 CC-SG 固件版本

1. 登录 CC-SG。
2. 在“帮助”菜单中，单击“关于 Raritan Secure Gateway”。出现一个弹出窗口，显示出固件的版本号。单击“确定”。
3. 如果版本不是最新，必须升级固件。可从 Raritan 网站下载固件升级文件，或从 Raritan CD 中获取。将固件升级文件保存到客户端 PC。

*注：必须先切换到“维护模式”下才能升级 CC-SG。详情参阅**第 11 章：系统维护**中的“维护模式”。*

4. 在“系统维护”菜单中，单击“维护模式”，然后单击“进入维护模式”。
5. 在“进入维护模式”屏幕中，在相应的字段中键入要对从 CC-SG 中注销的用户所显示的消息、要进入维护模式的分钟数，然后单击“确定”。
6. 单击确认对话框中的“确定”。
7. 当 CC-SG 进入维护模式时，会再出现一条确认消息。单击“确定”。
8. 从“系统维护”菜单中，单击“升级”。

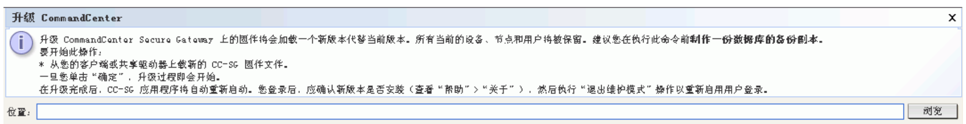


图 6 升级 CC-SG

9. 单击“浏览”，从出现的“打开”对话框中查找和选择固件升级文件，然后单击“打开”。
10. 在“升级 CommandCenter”屏幕中单击“确定”。

注：如果通过 zip 文件获得固件，请解压文件，并遵循自述文件中的说明。

检查和升级应用程序版本

检查和升级 CC-SG 应用程序，例如 Raritan Console (RC) 和 Raritan Remote Client (RRC)。

1. 从“管理”菜单中，单击“应用程序”。

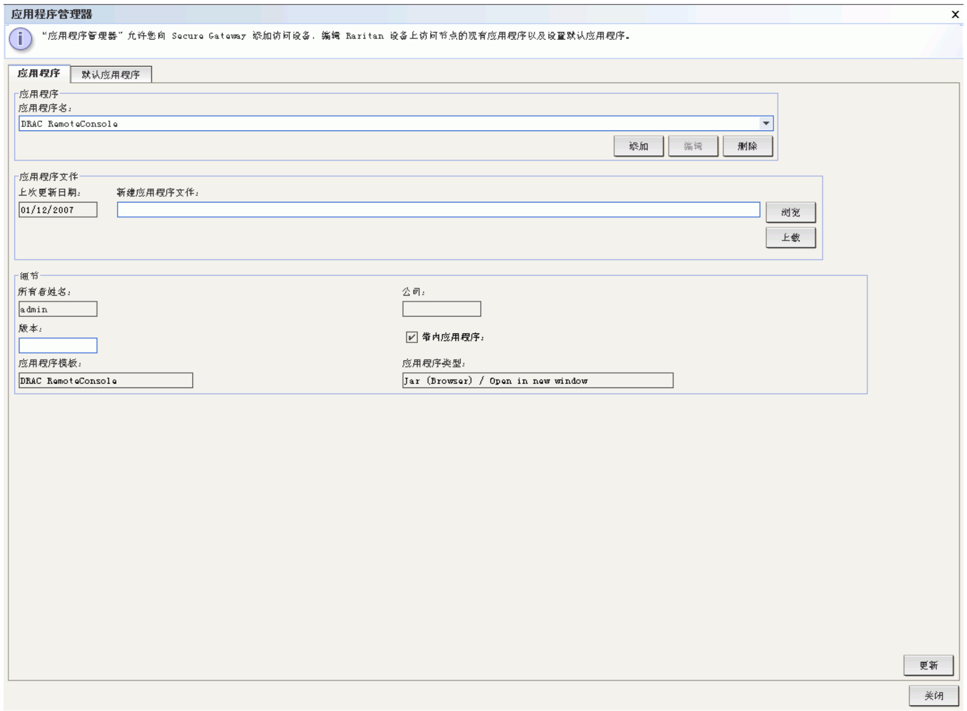


图 7 CC-SG 应用程序管理器

2. 单击“应用程序名称”下拉箭头并从列表中选择应用程序。记录“版本”字段中的数字。
3. 如果应用程序版本不是最新，必须升级应用程序。可从 Raritan 网站下载应用程序升级文件，或从 Raritan CD 中获取。将应用程序升级文件保存到客户端 PC。（有关所支持的应用程序版本完整列表，请参照 **http://www.raritan.com/support** 上的“兼容性矩阵”）。在“支持”页面上，单击“固件升级”，然后单击 **CommandCenter Secure Gateway**）。
4. 单击“应用程序名称”下拉箭头，从列表中选择要升级的应用程序。
5. 单击“浏览”，从出现的“打开”对话框中查找和选择应用程序升级文件，然后单击“打开”。
6. 应用程序名称将出现在“应用程序管理器”屏幕上的“新应用程序文件”字段内。
7. 单击“上载”。进度窗口会显示新的应用程序正被上载。完成后，出现新的窗口显示应用程序已被添加到 CC-SG 数据库，可用于配置和附加到特定端口。
8. 如果需要，请在“版本”字段中键入新的版本号。对于有些应用程序，“版本”字段会自动更新。
9. 单击“更新”。
10. 单击“关闭”关闭“应用程序管理器”屏幕。

关闭 CC-SG

如果 V1 设备启动后运行 CC-SG 时失去交流电源，则 V1 设备会记住其上次电源状态。一旦交流电源恢复后，V1 设备会自动重新启动。但是，如果 V1 设备在关闭状态下断开交流电源，则恢复交流电源后 V1 设备仍保持关机状态。

重要说明：不要按住 POWER 按钮强制关闭 CC-SG。建议采用以下程序关闭 CC-SG。

要关闭 CC-SG：

1. 卸掉前盖，坚定地按下 **POWER** 按钮。在 G1 设备上，**POWER** 按钮位于设备的后部。
2. 等待大约一分钟，CC-SG 会正常关机。

注：如果用户通过诊断控制台登录到 CC-SG，则 CC-SG 关机时会收到一条广播短消息。如果用户通过 Web 浏览器或 SSH 登录到 CC-SG，则 CC-SG 关机时不会收到一条广播短消息。

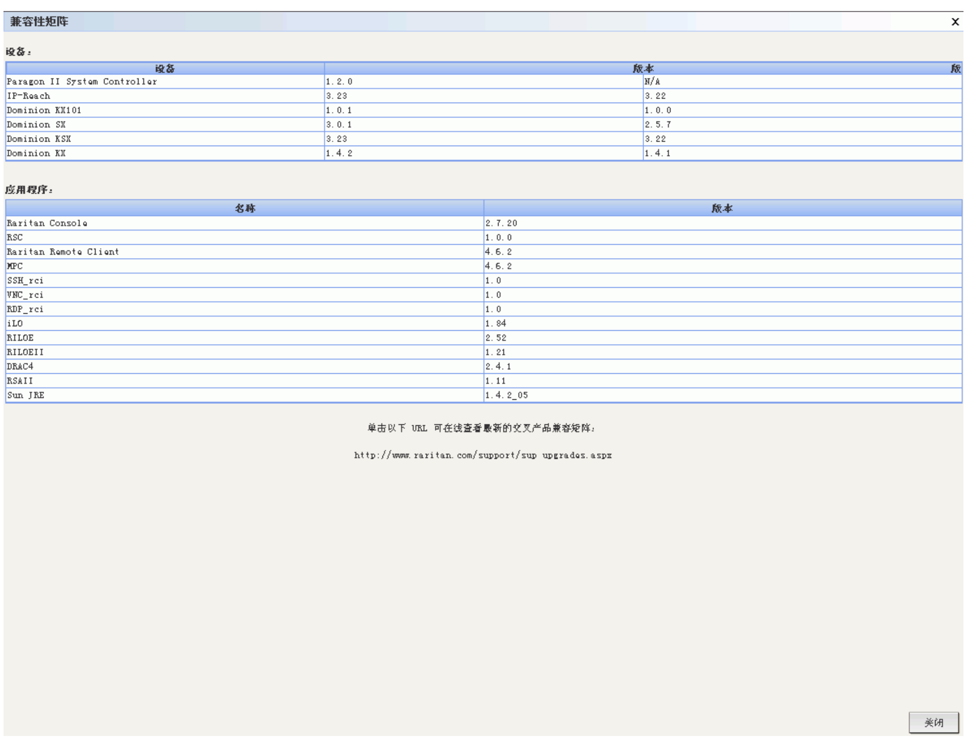
---

3. 如果要断开交流电源线，请先让关机过程完全结束，然后再拆掉电源线。这一点很有必要，可让 CC-SG 完成所有事务、关闭数据库并将磁盘置于断电的安全状态。

兼容性矩阵

兼容性矩阵列出与当前 CC-SG 版本兼容的 Raritan 设备固件版本以及设备软件版本。每次添加设备、升级设备固件或选择使用设备时，CC-SG 都会按此数据进行检查。如果固件或软件版本不兼容，在继续进行之前 CC-SG 将发出警告消息。每个 CC-SG 版本仅支持此次发行的 Raritan 设备当前和以前的固件版本。

- 从“管理”菜单中，单击“兼容性矩阵”。



设备	版本	版
Paragon II System Controller	1.2.0	N/A
IP-Reach	3.23	3.22
Dominion KX101	1.0.1	1.0.0
Dominion SX	3.0.1	2.5.7
Dominion KSX	3.23	3.22
Dominion KX	1.4.2	1.4.1

名称	版本
Raritan Console	2.7.20
RSC	1.0.0
Raritan Remote Client	4.6.2
MPC	4.6.2
SSH_rci	1.0
VNC_rci	1.0
RDP_rci	1.0
iLO	1.84
RILOE	2.52
RILOEII	1.21
DRAC4	2.4.1
RSAII	1.11
Sun JRE	1.4.2_05

图 8 兼容性矩阵

第 3 章：使用指导设置配置 CC-SG

准备使用指导设置配置 CC-SG

在继续进行 CC-SG 配置之前，必须先完成系统配置。

- 配置和安装 Dominion 系列以及 IP-Reach 设备（串行和 KVM 设备），包括分配 IP 地址和创建 CC-SG 管理员帐户。

指导设置概述

系统配置一旦完成后，指导设置可提供一种完成初始 CC-SG 配置任务的方法。“指导设置”接口引导完成定义关联、发现设备并添加到 CC-SG、创建设备组和节点组、创建用户组、将策略和权限指定给用户组以及添加用户。完成指导配置后，将始终可以个别地修改配置。

开始指导设置

在“管理”菜单中单击“指导设置”。出现“指导设置”窗口。窗口的左侧面板中以树形视图形式列出“指导任务”。窗口的右侧显示活动任务面板。

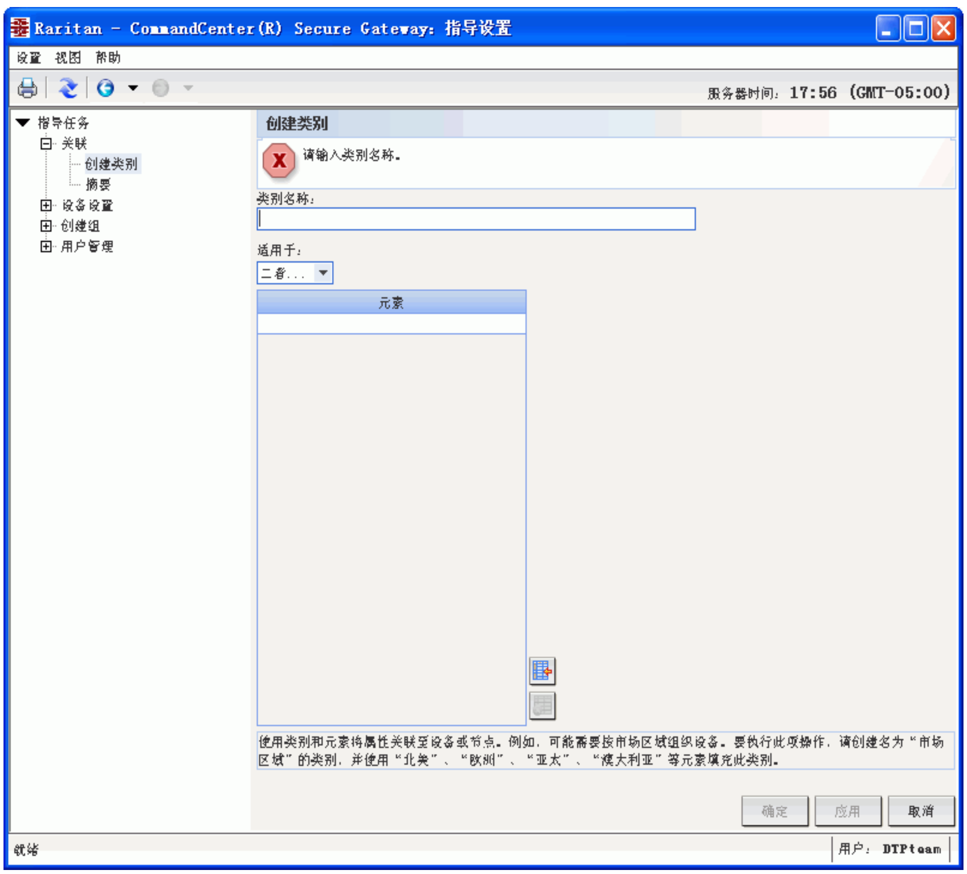


图 9 指导设置窗口

“指导设置”分成四个任务，将在以下小节分别予以介绍：

- 关联—定义类别和元素用于组织设备。
- 设备设置—发现网络中的设备并添加到 CC-SG。配置设备端口。
- 创建组—将 CC-SG 管理的设备和节点分类成组，并为每个组创建完整访问策略。
- 用户管理—将用户和用户组添加到 CC-SG，选择管理 CC-SG 内用户访问以及对设备和节点访问的策略和权限。

关联

可设置关联帮助组织 CC-SG 所管理的设备。每个关联包括一个类别（最高层的组织组）及其相关元素（类别的子集）。例如，要按照位置组织设备，则可创建一个名为“Location”的类别，以及为每个服务器位置命名的元素，例如“Philadelphia”、“纽约”和“新奥尔良”。

创建类别和元素

1. 在“指导设置”窗口中，默认的面板是“创建类别”。单击“关联”，然后单击左面板中的“创建类别”打开“创建类别”面板。

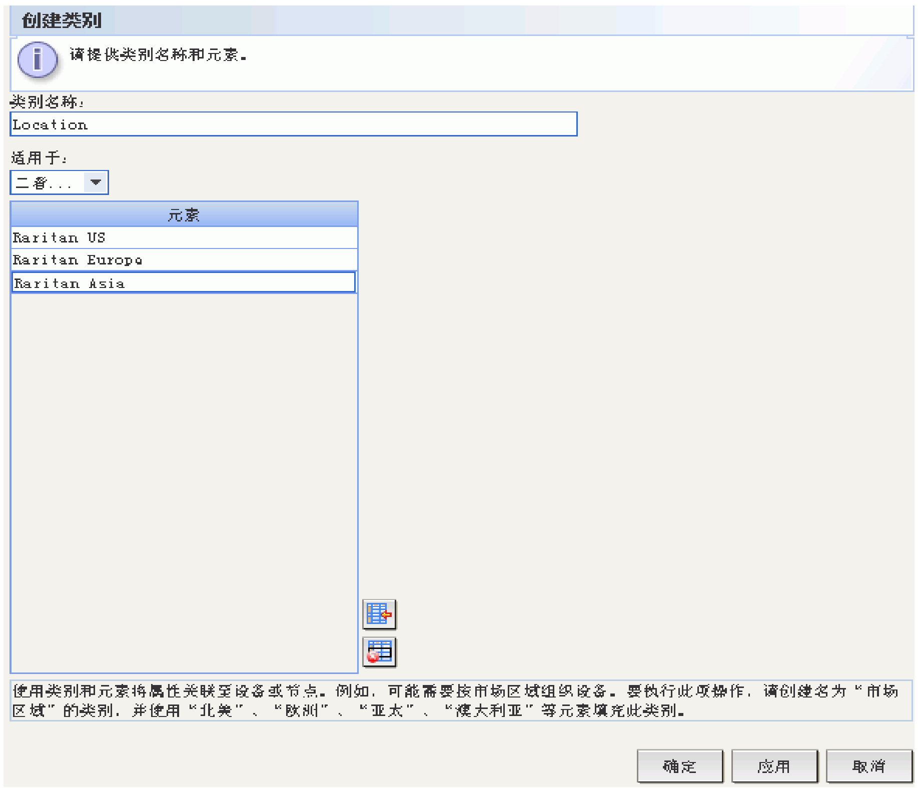


图 10 指导设置 – 创建类别和元素

2. 在“类别名称”字段中，键入希望按其来组织设备的类别名称，例如“Location”。
3. 在“适用于”字段中，可指示是否将类别可用于设备、节点或二者皆可。单击“适用于”下拉菜单，从列表中选择一个值。
4. 在“元素”表内，键入类别内一个元素的名称，例如“Raritan US”。

- 根据需要，单击添加新行图标  向“元素”表中添加多行。
- 要删除元素，请选择该行，然后单击删除行图标  从“元素”表内删除所选的元素。

5. 重复这些步骤，直到类别的所有元素都被添加到“元素”表中。
6. 如果想要创建其它类别，请单击“应用”保存该类别，然后重复本节中的步骤添加其它类别。
7. 创建类别和元素完成以后，单击“确定”。“关联摘要”面板显示一个所创建的类别和元素列表。
8. 单击“继续”开始下一个任务“设备设置”。按照下节所述的步骤操作。

设备设置

“指导设置”的第二个任务是“设备设置”。“设备设置”允许搜索和发现网络中的设备，并将其添加到 CC-SG。当添加设备时，可以对于每个类别选择一个元素与设备关联。

重要说明：在 CC-SG 配置期间，确保没有其他用户登录到设备。

发现和添加设备

1. 在“关联”任务结束后单击“继续”，就会打开“发现设备”面板。也可以单击“设备设置”，然后在左侧面板内“指导任务”树形视图内单击“发现设备”，即打开“发现设备”面板。

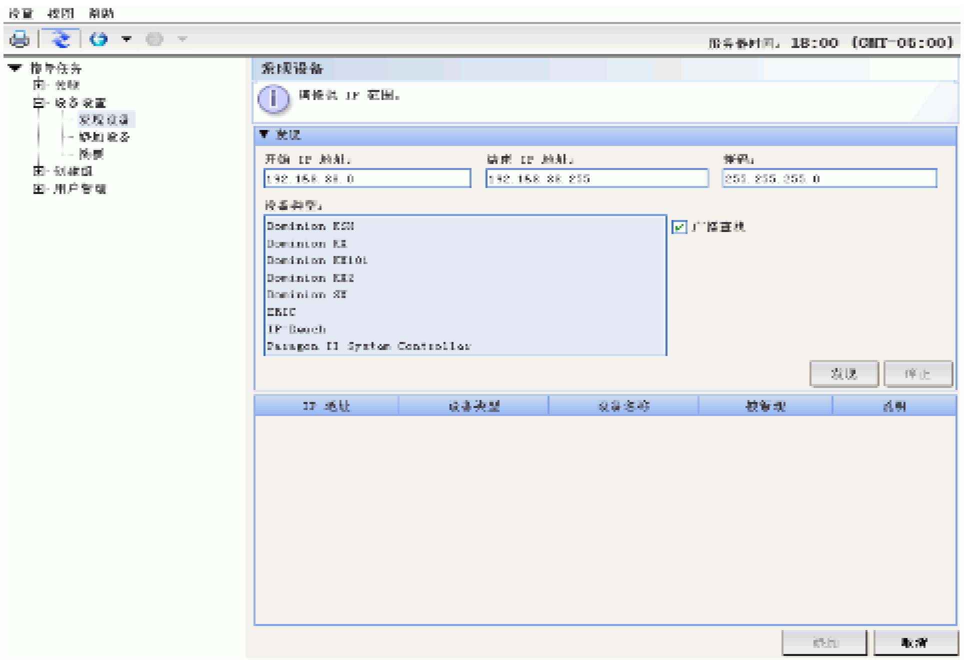


图 11 指导设置 – 发现设备

2. 在“开始地址”和“结束地址”字段中键入要搜索的设备的 IP 地址范围。
3. 在“掩码”字段中键入要搜索的设备的子网掩码。
4. 在“设备类型”列表中，在指定的范围内搜索想要搜索的设备类型。按住 **Ctrl** 键单击设备类型即可选择多个设备类型。
5. 如果在 CC-SG 所在的同一个子网内搜索设备，选中“广播查找”。取消选择“广播查找”即在所有子网内发现设备。
6. 单击“发现”。
7. 当发现操作完成后，将弹出确认消息。单击确认消息中的“确定”。

8. 如果 CC-SG 在指定的地址范围内发现指定类型的设备，则设备显示在“发现设备”面板底部的表内。单击面板顶部的黑色箭头可隐藏上面的部分，在面板的下面部分展开发现结果视图。

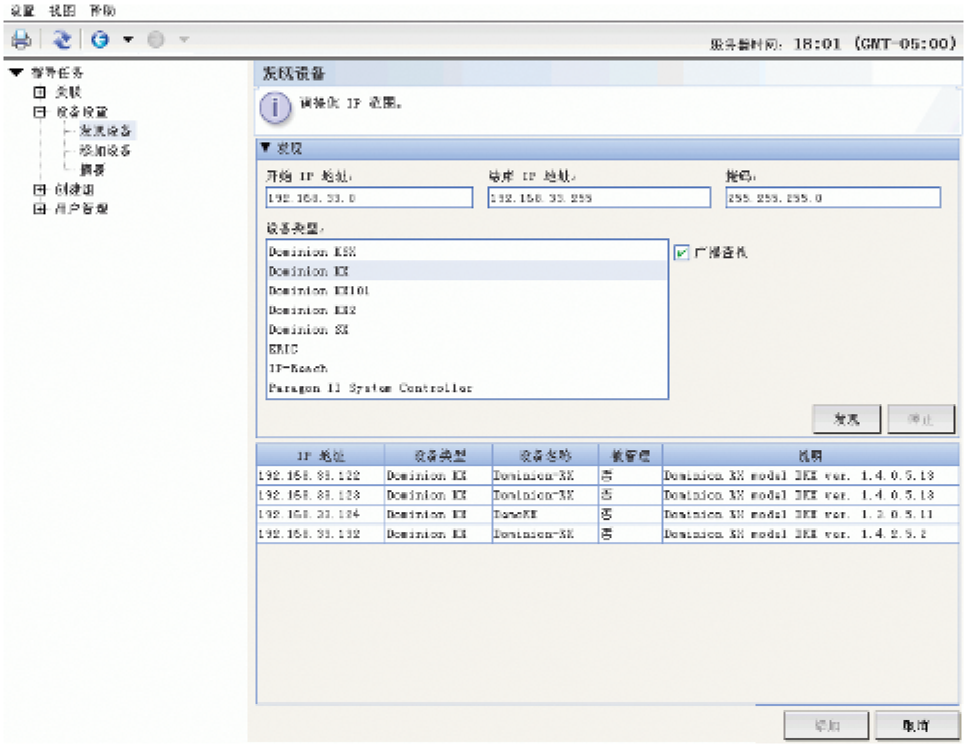


图 12 指导设置 – 设备发现结果

9. 在已发现的设备表内，选择要添加到 CC-SG 的设备，然后单击“添加”。打开“添加设备”面板。根据所添加的设备类型，“添加设备”面板略有不同。

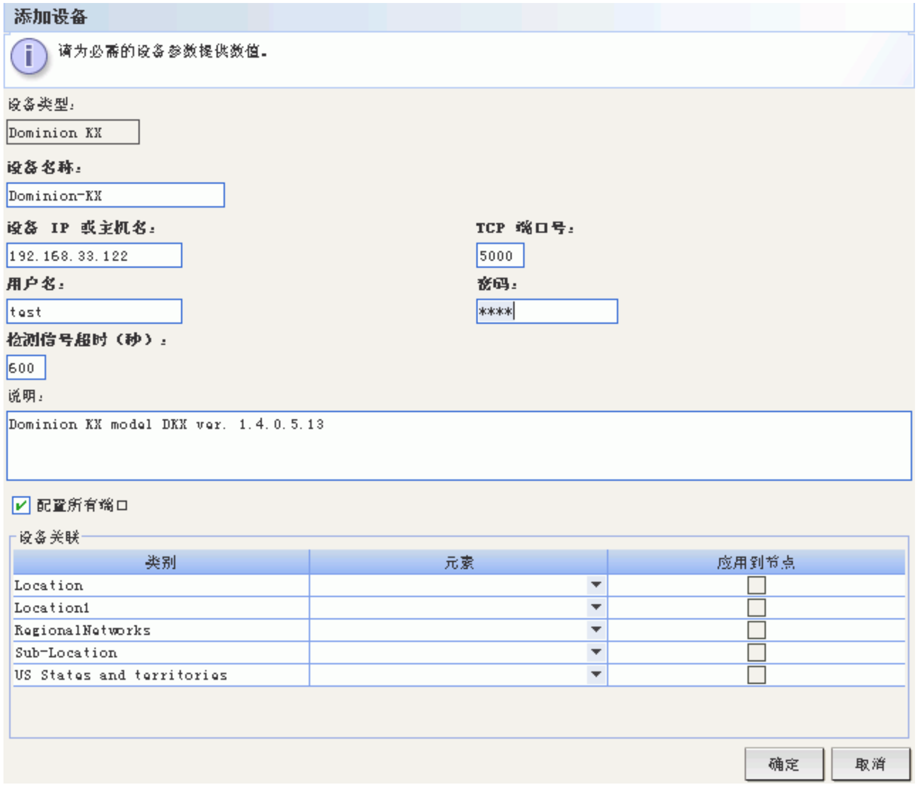


图 13 指导设置 – 添加设备

10. 在相应的字段中键入新信息，即可更改“设备名称”和“说明”。
11. 确认在准备将设备添加到 CC-SG 时所指定的 IP 地址显示在“设备 IP 或主机名”字段中，或者如果需要，在该字段中键入正确的地址。
12. 根据设备类型，“TCP 端口号”字段将自动填充。
13. 在相应的字段中键入在准备将设备添加到 CC-SG 时所创建的用户名和密码。在“检测信号超时”字段内，键入设备与 CC-SG 之间超时之前应经过的秒数。
15. 如果在添加 Dominion SX 设备并且希望允许对设备的本地访问， 请选中“本地访问：允许”复选框。如果不希望允许对设备的本地访问， 请清除“本地访问：允许”复选框。
16. 如果在手动添加 PowerStrip 设备，单击“端口数”下拉箭头，选择 PowerStrip 所含的出口个数。
17. 如果在添加 IPMI 服务器，在相应的字段中键入用于检测可用性的“时间间隔”以及“认证方法”（应与 IPMI 服务器上的配置相同）。
18. 如果希望在设备上配置所有可用端口，请选中“配置所有端口”复选框。CC-SG 将把设备上的所有端口添加到 CC-SG，并为每个端口创建一个节点。
19. 在面板底部的“设备关联”部分内，单击要指定给设备的每个类别相对应的“元素”栏内的下拉箭头，然后从列表中选择要与设备关联的元素。
20. 如果要将元素应用到设备以及设备上连接的节点，请选中“应用到节点”复选框。
21. 如果想要添加其它设备，请单击“应用”保存该设备，然后重复本节中的步骤添加其它设备。
22. 添加设备完成后，单击“确定”。“设备摘要”面板显示一个所添加的设备的列表。
23. 单击“继续”开始下一个任务“创建组”。按照下节所述的步骤操作。

创建组

“指导设置”的第三个任务是“创建组”。“创建组”允许定义设备组和节点组，并且指定每个组内包含的设备或节点集合。管理员管理类似设备和节点的组，而不是单个管理设备或节点，从而节省时间。

添加设备组和节点组

1. 在“设备设置”任务结束后单击“继续”，就会打开“设备组管理器”面板。也可以单击“创建组”，然后在左侧面板内“指导任务”树形视图内单击“添加设备组”，即打开“设备组管理器”面板。
2. 在“组名称”字段中，为要创建的设备组键入名称。
3. 将设备添加到组可通过两种方式：“选择设备”和“描述设备”。“选择设备”选项卡允许通过从可用设备列表中选择设备，从而选择将哪些设备指定给组。“描述设备”选项卡允许指定描述设备的规则，参数符合这些规则的设备将被添加到组中。

选择设备

a. 在“添加设备组”面板内单击“选择设备”选项卡。

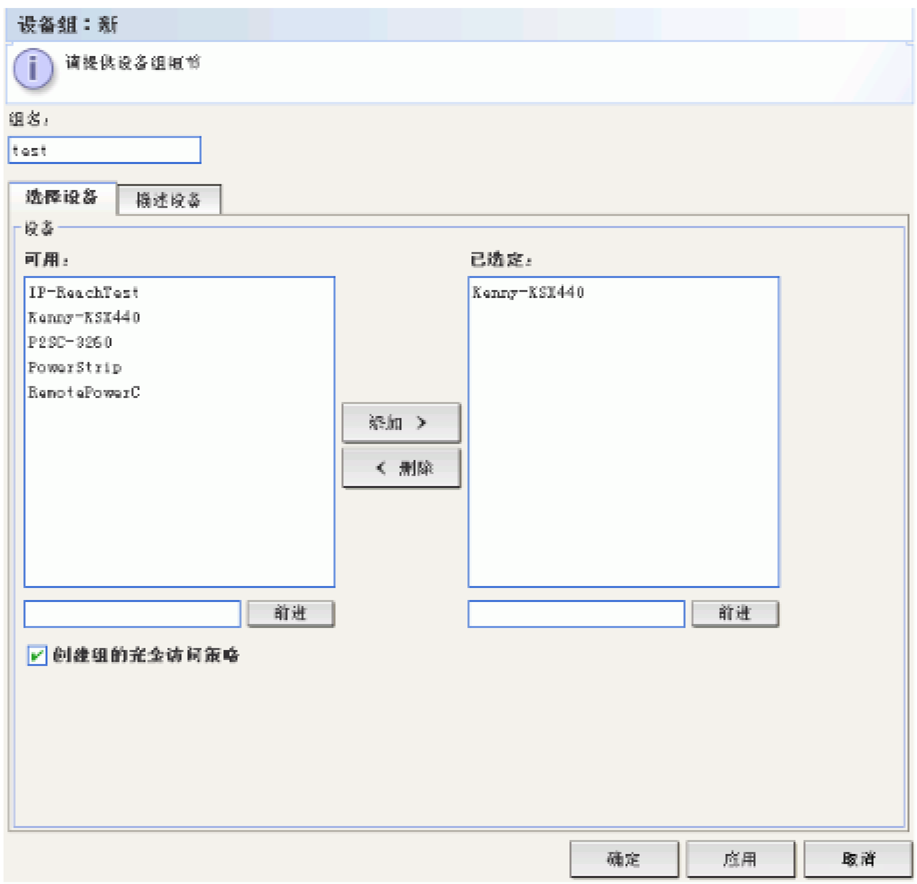


图 14 指导设置 – 添加设备组，选择设备

b. 在“可用”列表中选择要添加到组中的设备，然后单击“添加”将设备移到“已选定”列表中。“已选定”列表中的设备将被添加到组中。

- 如果需要从组中删除某个设备，请从“已选定”列表选择该设备名称，然后单击“删除”。
- 可在“可用”或“已选定”列表中搜索设备。在列表下面的字段中键入搜索术语，然后单击“执行”。

描述设备

a. 在“添加设备组”面板内单击“描述设备”选项卡。在“描述设备”选项卡中，可创建一个规则表来描述要指定到组中的设备。

b. 单击添加新行图标  向表中添加一行。

c. 双击为每列创建的单元格激活下拉菜单。选择要从每个列表中使用的规则组件。

d. 要为此设备组创建一个策略允许对组内所有节点和设备在所有时间拥有控制权限访问，则选中“创建组的完全访问策略”。

e. 如果想要添加其它设备组，请单击“应用”保存该组，然后重复本节中的步骤添加其它设备组。

f. 添加设备组完成后，单击“确定”。打开“节点组管理器”面板。也可以单击“创建组”，然后在左侧面板内“指导任务”树形视图内单击“添加节点组”，即打开“节点组管理器”面板。

g. 在“组名称”字段中，为要创建的节点组键入名称。

h. 将节点添加到组可通过两种方式：“选择节点”和“描述节点”。“选择节点”部分允许通过从可用设备列表中选择节点，从而选择将哪些节点指定给组。“描述节点”部分允许指定描述节点的规则，参数符合这些规则的节点将被添加到组中。

选择节点

a. 在“添加节点组”面板内单击“选择节点”选项卡。

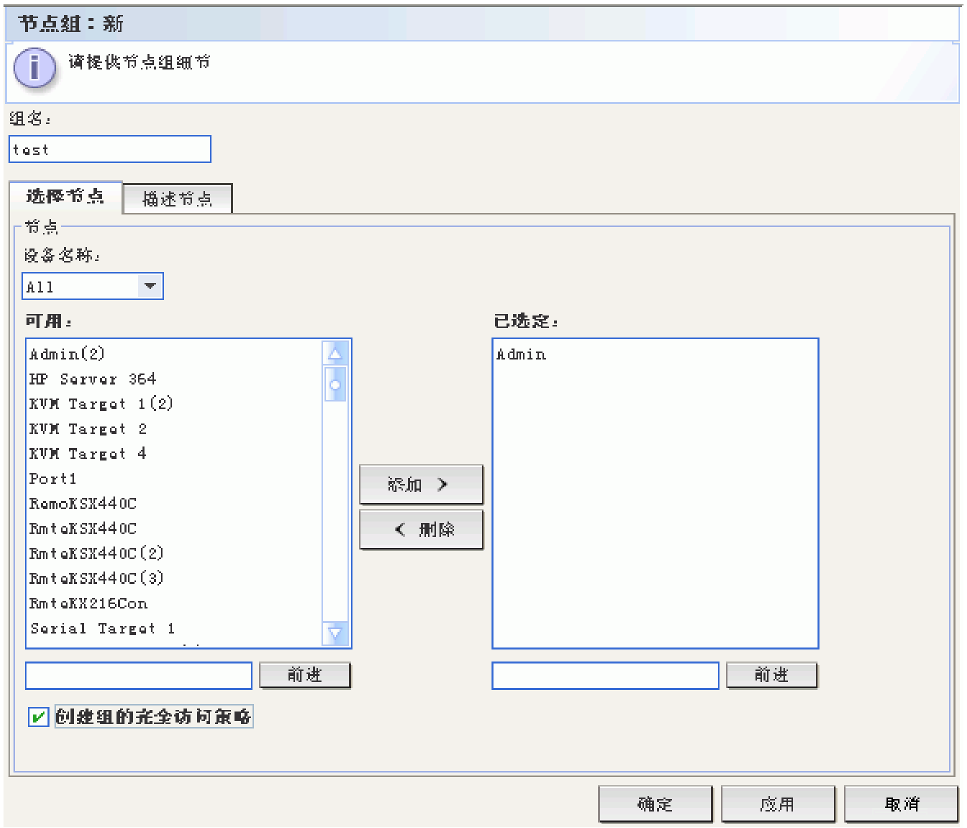


图 15 指导设置 – 添加节点组，选择节点

b. 在“可用”列表中选择要添加到组中的节点，然后单击“添加”将节点移到“已选定”列表中。“已选定”列表中的节点将被添加到组中。

c. 如果需要从组中删除某个节点，请从“已选定”列表选择该节点名称，然后单击“删除”。

e. 可在“可用”或“已选定”列表中搜索节点。在列表下面的字段中键入搜索术语，然后单击“执行”。

描述节点

a. 在“描述节点组”面板内单击“选择节点”选项卡。在“描述节点”选项卡中，可创建一个规则表来描述要指定到组中的节点。

b. 单击添加新行图标  向表中添加一行。

c. 双击为每列创建的单元格激活下拉菜单。选择要从每个列表中使用的规则组件。详情参见第 8 章：策略。

d. 要为此节点组创建一个策略允许对组内所有节点在所有时间拥有控制权限访问，则选中“创建组的完全访问策略”。

e. 如果想要添加其它节点组，请单击“应用”保存该组，然后重复本节中的步骤添加其它节点组。

f. 添加节点组完成后，单击“确定”。“组摘要”面板显示一个所添加的组的列表。

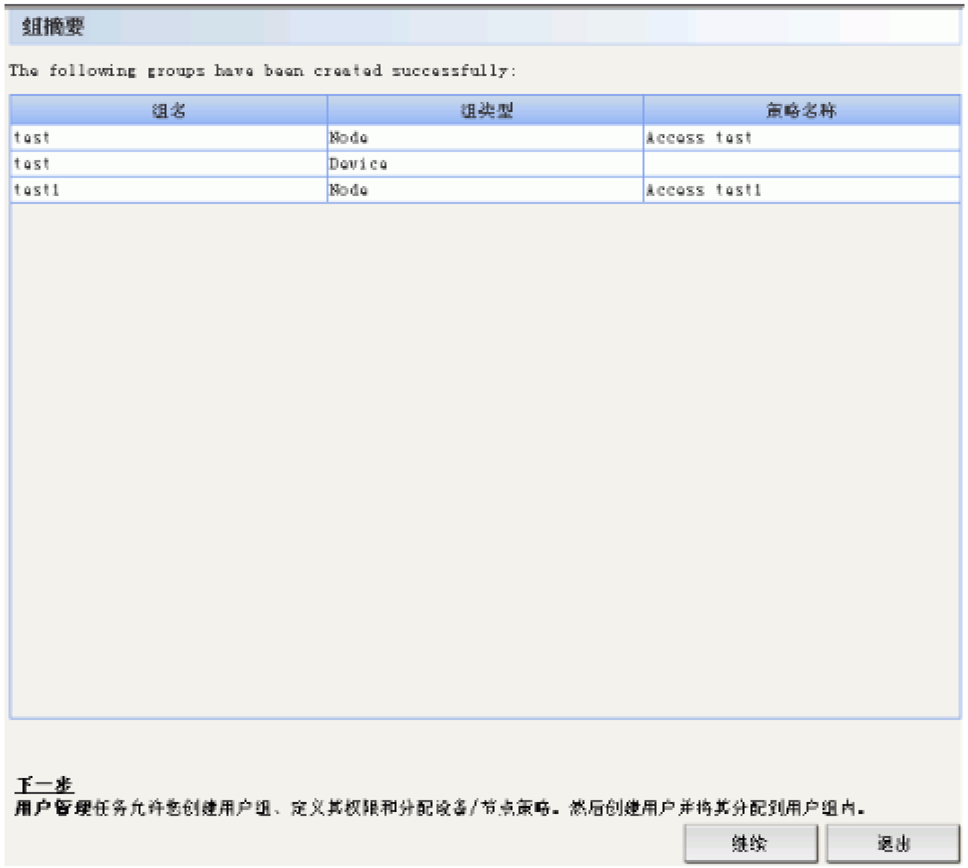


图 16 指导设置 – 组摘要

g. 单击“继续”开始下一个任务“用户管理”。按照下节所述的步骤操作。

用户管理

“指导设置”的第四个任务是“用户管理”。“用户管理”允许选择“权限”和“策略”来管理用户组的访问和活动。权限规定用户组内的成员能在 CC-SG 内进行哪些活动。策略规定用户组的成员可查看和修改哪些设备和节点。策略基于类别和元素之上。创建用户组以后，可定义单个用户并添加到用户组。

添加用户组和用户

1. 在“创建组”任务结束后单击“继续”，就会打开“添加用户组”面板。也可以单击“用户管理”，然后在左侧面板内“指导任务”树形视图内单击“添加用户组”，即打开“添加用户组”面板。
2. 在“用户组名称”字段中，为要创建的用户组键入名称。
3. 在“说明”字段内为此用户组键入说明。
4. 单击“权限”选项卡，然后选择要分配到用户组的“权限”或 CC-SG 活动类型所对应的复选框。

5. 在“节点访问”部分，可指定用户组是否有权访问“带内”和“带外”节点以及“电源管理”功能。对于要指定给组的访问类型，选中其对应的复选框。

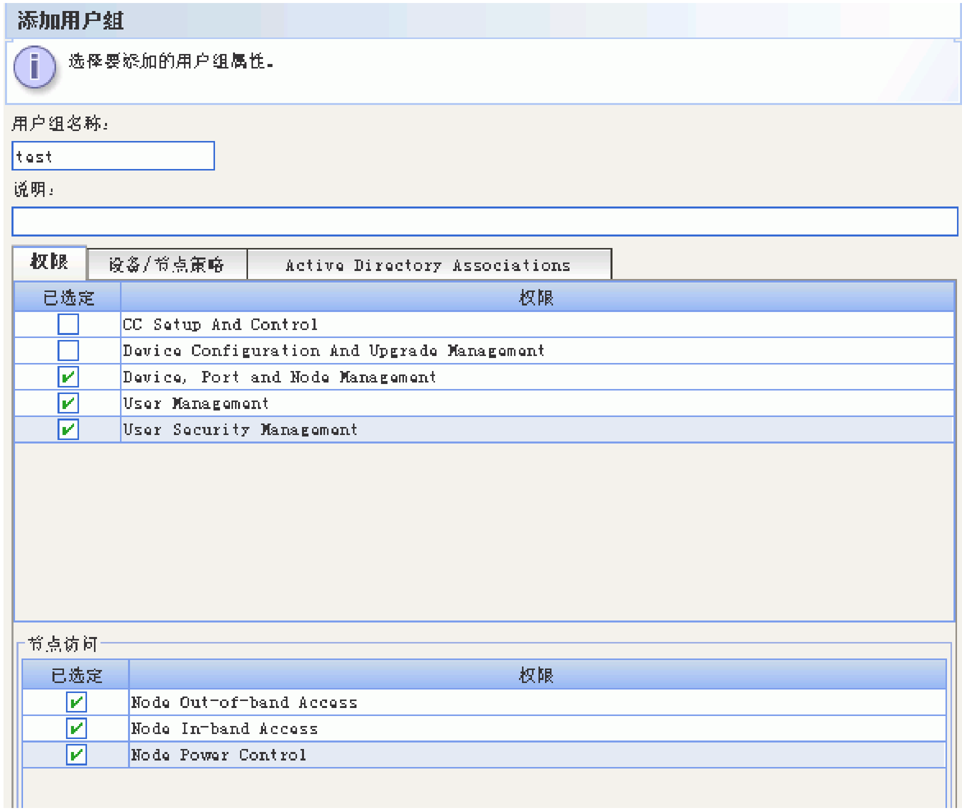


图 17 添加用户组 – 权限

6. 单击“策略”选项卡。

7. 在“所有策略”列表中，选择要指定给用户组的策略，然后单击“添加”将策略移到“已选定策略”列表中。“已选定策略”列表中的策略将被指定给用户组。重复此步骤将其它策略添加到用户组。



图 18 添加用户组 – 策略

8. 如果需要从用户组中删除某个策略，请从“已选定策略”列表选择该策略名称，然后单击“删除”。
9. 要将远程认证用户与 Active Directory 模块关联，请单击“Active Directory 关联”选项卡。对于要与用户组关联的 Active Directory 模块，选中其对应的复选框。
10. 如果想要添加其它用户组，请单击“应用”保存该组，然后重复本节中的步骤添加其它用户组。
11. 添加用户组完成后，单击“确定”。打开“添加用户”面板。也可以单击“用户管理”，然后在左侧面板内“指导任务”树形视图内单击“添加用户”，即打开“添加用户”面板。
12. 在“用户名”字段中，键入要添加用户的名称，此名称将用于登录 CC-SG。
13. 如果想要此用户能够登录 CC-SG，则选中“登录已启用”复选框。
14. 只有在用户需要在服务器外进行认证（例如 TACACS+、RADIUS、LDAP 或 AD），选中“远程认证”复选框。如果使用远程认证，则不需要密码。当“远程认证”被选中时，“新密码”和“重新键入新密码”字段被禁用。
15. 在“新密码”和“重新键入新密码”字段中，键入用户登录 CC-SG 时所用的密码。
16. 如果想要强制用户在下次登录时更改所分配的密码，则选中“强制下次登录时更改密码”复选框。
17. 如果想要指定强制用户多久更改一次密码，则选中“强制定期更改密码”复选框。
18. 在“到期周期（天）”字段中，键入强制用户更改密码之前可使用的天数。

19. 在“电子邮件地址”字段内，键入用户的电子邮件地址。
20. 单击“用户组”下拉箭头，从列表中选择要将用户分配给哪个用户组。
21. 如果想要添加其它用户，请单击“应用”保存该用户，然后重复本节中的步骤添加其他用户。
22. 添加用户完成后，单击“确定”。“用户摘要”面板显示一个所添加的用户组和用户的列表。

第 4 章：创建关联

关联

可设置关联帮助组织 CC-SG 所管理的设备。每个关联包括一个类别（最高层的组织组）及其相关元素（类别的子集）。例如，可能有 Raritan 设备管理位于纽约、Philadelphia 和新奥尔良数据中心内的目标服务器。则可以设置一个关联按照位置组织此设备。然后，可自定义 CC-SG 在其界面中按照所选的类别（“Location”）显示 Raritan 设备和节点及其关联的元素（“纽约”、“Philadelphia”和“新奥尔良”）。下图为用此示例创建的自定义视图。可以自定义 CC-SG 根据需要来组织和显示服务器。

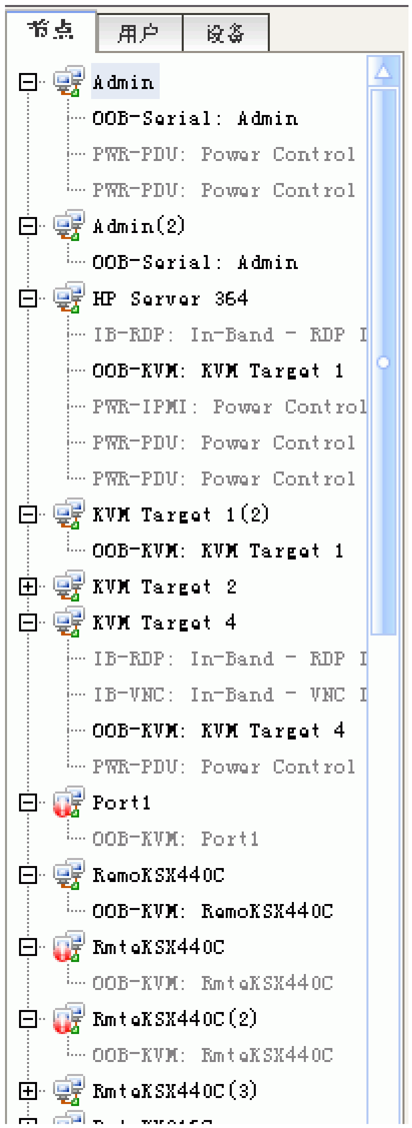


图 19 CC-SG 关联示例

关联术语

请阅读以下定义来了解关联的含义：

- **关联**——类别、类别元素以及节点和设备之间的一种关系。例如，想要将“Location”类别与一个设备进行关联。应先创建关联或以后编辑关联，然后再在 CC-SG 中添加设备和端口。
- **类别**——包含一系列称为“元素”的值的变量。比如类别“Location”可含有“New York City”和“Philadelphia”等元素。再比如类别“OS 类型”可含有“Windows”、“Unix”或“Linux”等元素。将设备添加到 CC-SG 时，将会把此信息与其关联。
- **元素**——类别的值。例如，“New York City”元素属于“Location”类别。
- **设备**——CC-SG 所管理的 Raritan 设备，例如 Dominion KX、Dominion SX、Dominion KSX、IP-Reach、Paragon II System Controller、Paragon II UMT832 with USTIP 等。这些设备控制与其相连的目标系统或节点。
- **节点**——CC-SG 可访问和管理的目标系统或服务器。在 CC-SG 中单击节点即可通过接口来访问和管理节点。

关联——定义类别和元素

Raritan 设备和节点按照类别和元素进行组织。每个类别/元素对被分配到一个设备、节点或同时二者。因此，在 CC-SG 中添加 Raritan 设备之前，需要先定义类别和元素。

类别就是相似元素的组。例如，要按照位置组织 Raritan 设备，则可创建一个名为“Location”的类别，包含一系列的元素，例如“Philadelphia”、“纽约”和“新奥尔良”。

策略也使用类别和元素来控制用户对服务器的访问。例如，类别/元素对“Location/纽约”可用于创建一个策略来控制用户对位于纽约的服务器的访问。

关于类别和元素的关联配置，常见示例如下：

类别	元素
Location	纽约、Philadelphia、新奥尔良
OS 类型	Unix、Windows、Linux
部门	销售、IT、工程

关联配置要保持简单，以满足服务器/节点组织目标和用户访问目标的需要。一个节点只能被分配到一个类别中的单个元素。例如，一个目标服务器不能同时被分配到“OS 类型”类别的“Windows”和“Unix”元素。

在系统中如果服务器类似并需要随机组织，则以下方法会比较实用：

类别	元素
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

在将设备和节点添加到 CC-SG 时，将其链接到预先定义的类别和元素上。在创建节点和设备组并为其分配策略时，将会使用类别和元素来定义哪些节点和设备属于哪个组。

如何创建关联

创建关联可通过两种方式：“指导设置”和“关联管理器”。

- “指导设置”将多种配置任务合并到一个自动化界面中。在初始 CC-SG 配置时推荐采用这种方式。完成指导配置后，将始终可以个别地修改配置。详情参阅第 3 章：使用指导设置配置 CC-SG。
- “关联管理器”仅允许操作关联，而不能自动执行任何配置任务。有关详细信息，请参阅下页上的“关联管理器”部分。

关联管理器

“关联管理器”允许添加、编辑或删除类别和元素。

添加类别

1. 从“关联”菜单中，单击“关联”。出现“关联管理器”屏幕。

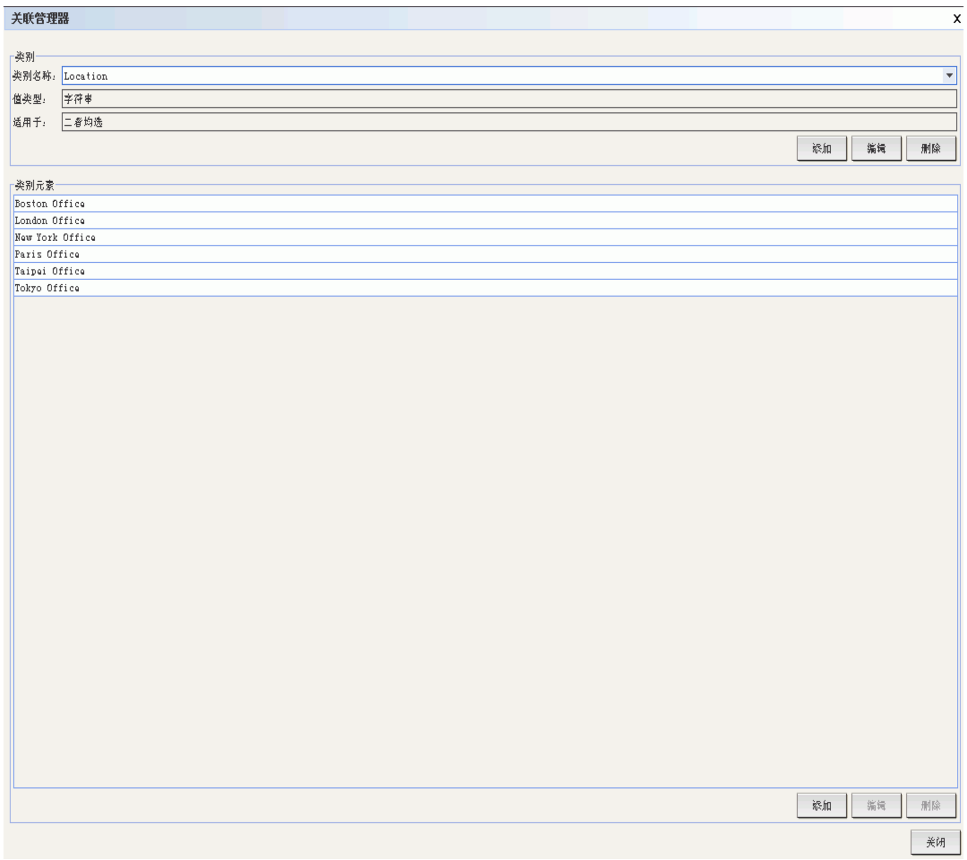


图 20 关联管理器屏幕

2. 在“类别”面板中单击“添加”以添加新类别。出现“添加类别”窗口。

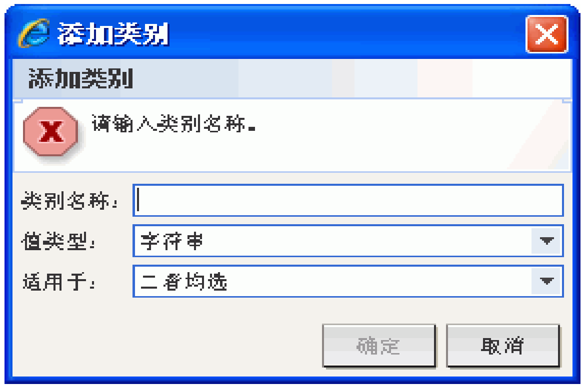


图 21 添加类别窗口

3. 在“类别名称”字段内键入类别名称。最长为 31 个字符。
4. 单击“值类型”下拉箭头，选择一个值类型“字符串”或“整数”。
5. 单击“适用于”下拉箭头，选择此类别适用的设备类型：“设备”、“节点”或“二者均选”。
6. 单击“确定”创建新类别，或单击“取消”不创建退出。在“类别名称”字段内出现新类别的名称。

编辑类别

1. 从“关联”菜单中，单击“关联”。出现“关联管理器”屏幕。
2. 单击“类别名称”下拉箭头并选择要编辑的类别。
3. 在屏幕上的“类别”面板中单击“编辑”以编辑类别。出现“编辑类别”窗口。

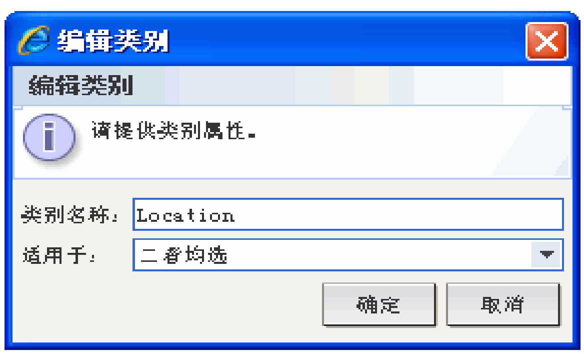


图 22 编辑类别窗口

4. 在“类别名称”字段内键入新类别的名称。
5. 单击“适用于”下拉箭头更改此类别是否适用于“设备”、“节点”或“二者均选”。请注意字符串值不能更改为整数值，反之亦然。如果必须进行此类型的更改，请删除类别，然后再添加一个全新的类别。
6. 单击“确定”保存更改。在“类别名称”字段内出现更新类别的名称。

删除类别

删除一个类别将会删除此类别内创建的所有元素。刷新屏幕后或用户注销再登录到 CC-SG 后，被删除的类别将不再出现于“节点”或“设备”树内。

1. 从“关联”菜单中，单击“关联”。出现“关联管理器”屏幕。
2. 单击“类别名称”下拉箭头并选择要删除的类别。
3. 在屏幕上的“类别”面板中单击“删除”以删除类别。出现“删除类别”窗口。

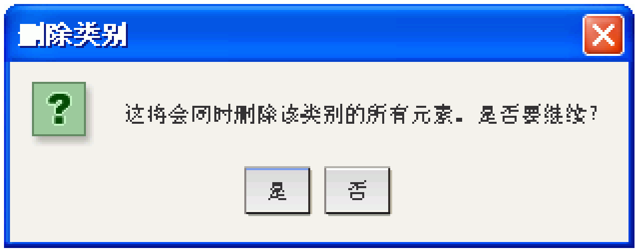


图 23 删除类别窗口

4. 单击“是”删除该类别。

添加元素

1. 从“关联”菜单中，单击“关联”。出现“关联管理器”屏幕。

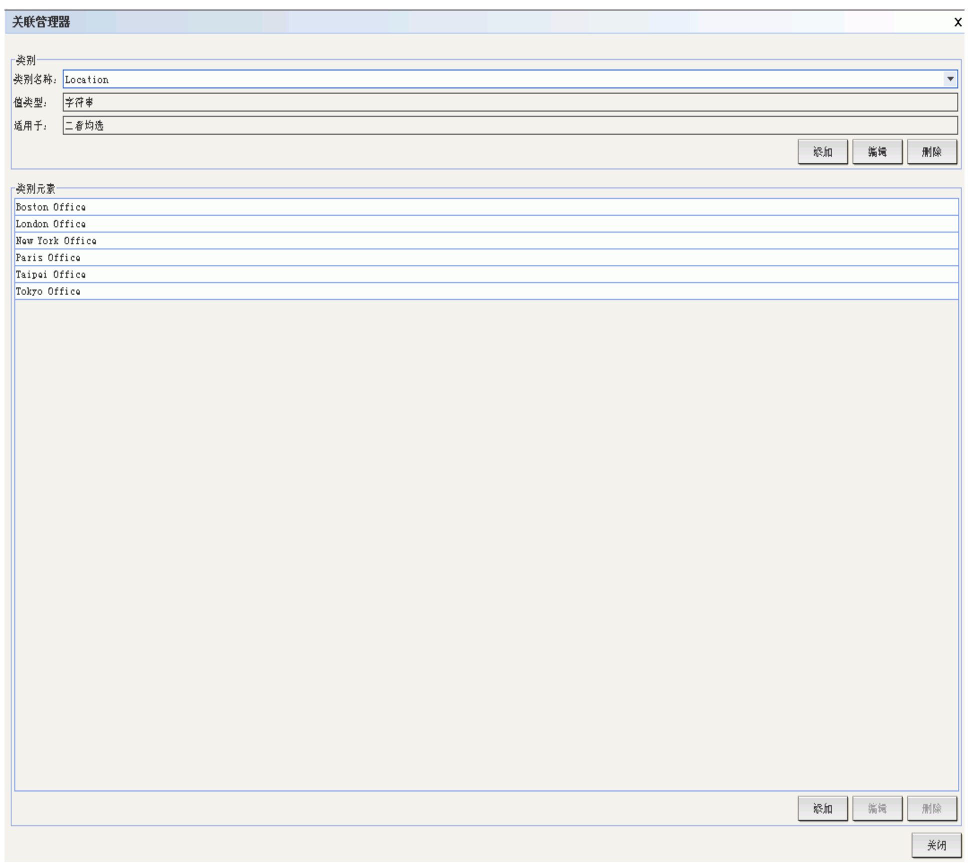


图 24 关联管理器屏幕

2. 单击“类别名称”下拉箭头并选择要添加新元素的类别。

3. 在“类别元素”面板中单击“添加”以添加新元素。出现“添加元素”窗口。

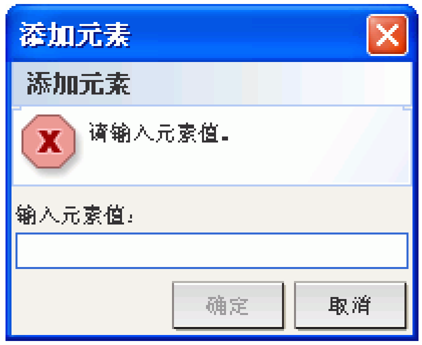


图 25 添加元素窗口

4. 在“输入元素值”字段内键入新元素的名称。
5. 单击“确定”添加元素，或单击“取消”退出窗口。新元素出现在“类别元素”面板内。

编辑元素

1. 从“关联”菜单中，单击“关联管理器”。出现“关联管理器”屏幕。
2. 单击“类别名称”下拉箭头并选择要编辑其元素的类别。
3. 从“类别元素”列出中选择要编辑的元素，然后单击“类别元素”面板中的“编辑”。出现“编辑元素”窗口。

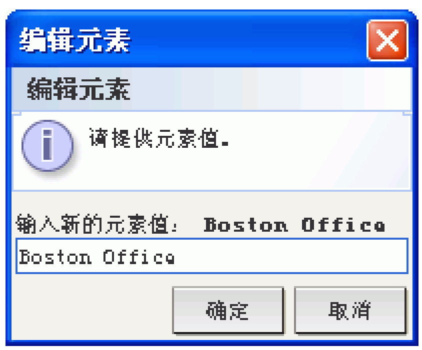


图 26 编辑元素窗口

4. 在“输入新的元素值”字段内键入元素的新名称。
5. 单击“确定”更新元素，或单击“取消”关闭窗口。新元素名称出现在“类别元素”列表内。

删除元素

删除元素将从所有关联中删除该元素，使关联字段变空。

1. 从“关联”菜单中，单击“关联”。出现“关联管理器”屏幕。
2. 单击“类别名称”下拉箭头并选择要删除其元素的类别。
3. 从“类别元素”列出中选择要删除的元素，然后单击“类别元素”面板中的“删除”。出现“删除元素”窗口。

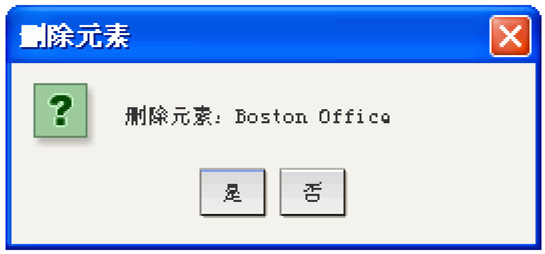


图 27 删除元素窗口

4. 单击“是”删除元素，或单击“否”关闭窗口。元素名称从“类别元素”列表内删除。

注：删除元素将从所有设备和节点类别关联中删除该元素，使所有预先关联的元素字段变空。

此页专门留白。

第 5 章：添加设备和设备组

必须先将 Raritan 设备（例如 Dominion 系列设备和 IP-Reach 设备）添加到 CC-SG，然后才能使用 CC-SG 对其进行配置和管理。“设备”菜单提供设备和端口相关的所有功能。在“设备”选项卡内右键单击设备或端口，并从出现的菜单中进行选择，也可访问部分功能。

*注：要配置 iLO/RILOE 设备、IPMI 设备、Dell DRAC 设备、IBM RSA 设备或其它“一般”设备，请使用“添加节点”菜单将这些项添加为连接接口。详情参见**第 6 章：配置节点和接口**。*

设备选项卡

单击“设备”选项卡显示“设备”树。

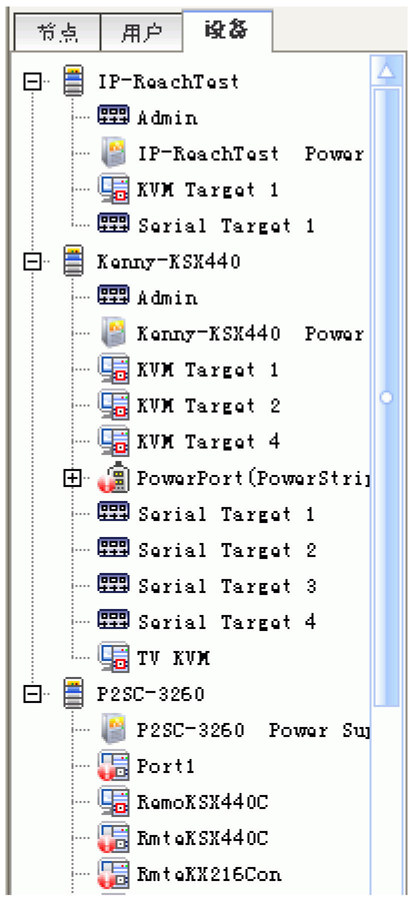


图 28 设备树

“设备”选项卡显示出设备及其配置的端口集合。端口内嵌于所属的设备之下。在列表中含有配置端口的设备旁边有一个 + 符号。单击 + 符号展开或隐藏端口列表。

设备和端口图标

为了便于识别，KVM、串行和电源设备和端口在设备树上有不同的图标。将鼠标指针停留在设备树内的图标上，即可看到有关该设备或端口信息的工具提示。

图标	含义
	设备可用
	KVM 端口可用或已连接
	KVM 端口不活动
	串口可用
	串口不可用
	设备暂停
	设备不可用
	配电盘
	出口端口

单击“设备”选项卡中的一个设备，出现“设备配置文件”屏幕，显示所选设备的相关信息。

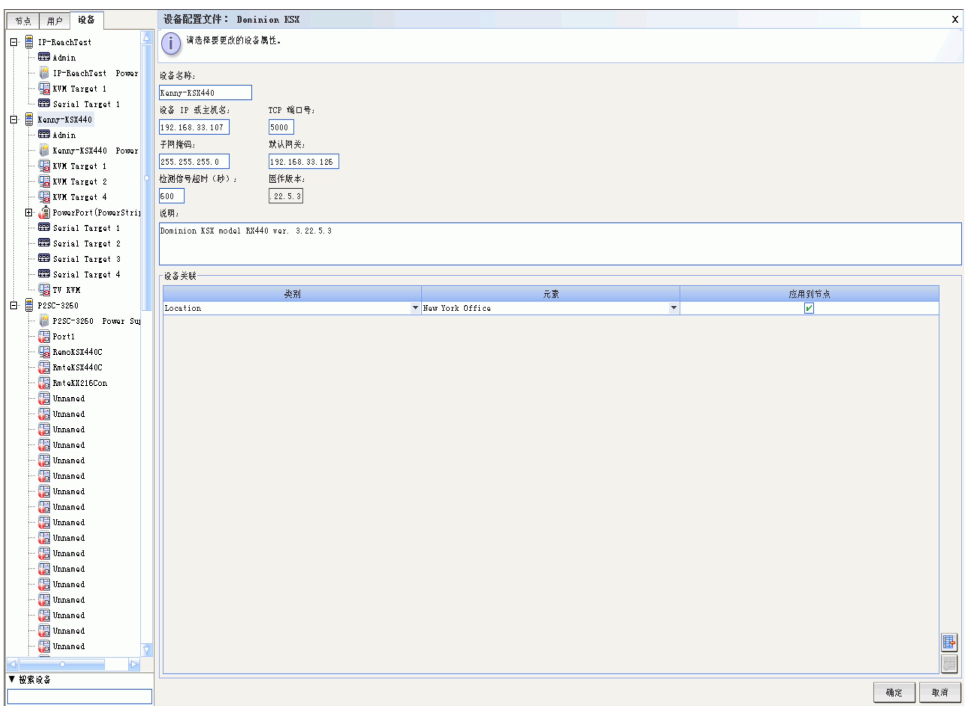


图 29 设备选项卡和设备配置文件

搜索设备

“设备”选项卡允许在树内搜索设备。搜索结果中仅返回设备，而不包括端口名称。搜索方法可在“我的配置文件”屏幕中配置，如**第 7 章：添加和管理用户和用户组**所述。

要搜索设备，在设备树底部的“搜索设备”字段中键入搜索字符串，然后按**回车**键。在搜索字符串中支持通配符：

通配符	说明
?	表示任何字符。
[-]	表示范围内的字符。
*	表示零个或多个字符。

例如：

示例	说明
KX?	查找 **KX1** 和 **KXZ**，但不查找 **KX1Z**。
KX*	查找 **KX1**、**KX**、**KX1** 和 **KX1Z**。
KX[0-9][0-9]T	查找 **KX95T** 和 **KX66T**，但不查找 **KXZ** 和 **KX5PT**。

重要事项！很多菜单栏命令可通过快捷菜单进行访问，即右键单击设备树内的设备或端口，然后从显示的快捷菜单中选择命令。

添加设备

必须先将设备添加到 CC-SG，然后才能配置端口，并通过这些端口将带外接口添加到节点。“添加设备”用于添加属性已知并可以向 CC-SG 提供的设备。

要将设备添加到 CC-SG：

1. 在“设备”菜单中，单击“设备管理器”，然后单击“添加设备”。出现“添加设备”屏幕。

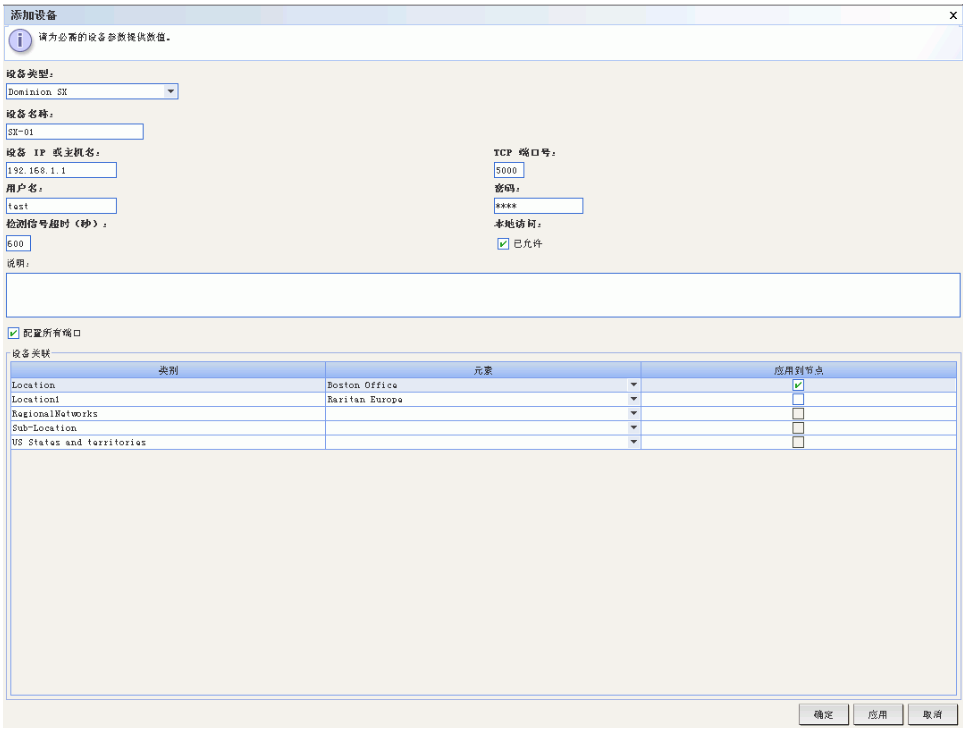


图 30 添加设备屏幕

2. 单击“设备类型”下拉箭头，从列表中选择要添加的设备类型。如果选择“PowerStrip”，则看到的“添加设备”屏幕会略有不同。

添加 KVM 或串行设备

1. 在“设备名称”字段内键入设备的名称。
2. 在“设备 IP 或主机名”字段中键入设备的 IP 地址或主机名。对于主机名规则，参见**第 1 章：简介**中的**“术语/缩略语”**。
3. 在“TCP 端口号”字段中键入与设备通信所用的 TCP 通信端口。对于大多数 Raritan 设备来说，默认的端口号都是 5000。
4. 在“用户名”字段中键入登录此设备所用的名称。如果按照《Raritan 数字解决方案部署指南》准备添加到 CC-SG 中的设备，请为在设备上配置的 CC-SG 管理用户键入用户名。
5. 在“密码”字段中键入访问此设备需要的密码。如果按照《Raritan 数字解决方案部署指南》准备添加到 CC-SG 中的设备，请为在设备上配置的 CC-SG 管理用户键入密码。
6. 在“检测信号超时（秒）”字段内键入新设备与 CC-SG 之间超时之前经过的时间秒）。
7. 根据需要，如果要此设备在受到 CC-SG 管理时还允许用户对其进行直接访问，则选中“本地访问”下面的“允许”。

8. 在“说明”字段内为此设备键入可选的简短说明。
9. 如果要自动将此设备上的所有端口添加到“设备”选项卡，并在“节点”选项卡内为设备上的每个端口创建一个节点，则选中“配置所有端口”。将使用匹配的名称配置相应的节点和端口。如果在添加设备时选中，则为每个端口创建一个新节点，并为该节点创建一个带外接口。
10. 可配置一个类别和元素列表，更好地描述和组织此设备以及与其相连的节点。详情参见第 4 章：创建关联。

    要配置**类别**和**元素**：

    a. 对于每个列出的类别，单击“元素”下拉菜单，然后从列表中选择要应用到设备的元素。对于不想用的类别，从“元素”字段中选择空白项。

    b. 如果要将元素分配到相关节点以及设备上，则选中“应用到节点”复选框。

    如果看不到要使用的类别或元素值，可通过“关联”菜单进行添加。详情参见**第 4 章：创建关联**。

11. 配置此设备完成后，单击“应用”添加此设备并打开一个空白的“添加设备”屏幕，可继续添加设备。或者，单击“确定”添加此设备而不继续显示新的“添加设备”屏幕。
12. 如果设备的固件版本与 CC-SG 不兼容，将出现警告消息询问是否继续。单击“是”将设备添加到 CC-SG。将设备添加到 CC-SG 以后可升级设备固件。请参阅本章后面的“升级设备”部分。

添加 PowerStrip 设备

添加 PowerStrip 设备时，可允许 CC-SG 自动配置其出口。出口配置以后，即可通过将电源接口添加到节点，将每个出口关联到它提供电源的节点。详情参见第 6 章：配置节点和接口。也可选择不让 CC-SG 配置出口，而是稍后由自己配置。

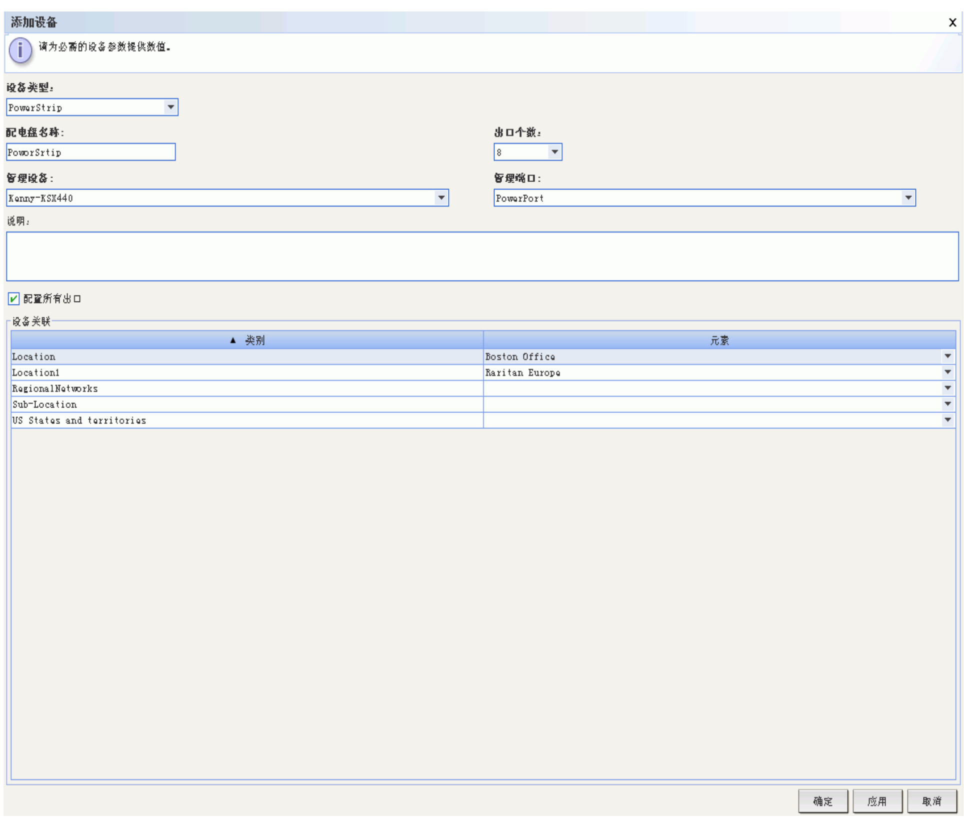


图 31 添加 PowerStrip 设备

1. 在“配电盘名称”字段内键入此配电盘的名称。
2. 单击“出口个数”下拉菜单，从列表中选择配电盘包含的出口个数。
3. 单击“管理设备”下拉菜单，从列表中选择管理此配电盘的设备。
4. 单击“管理端口”下拉菜单，选择此配电盘所连接的管理设备上的端口。
5. 在“说明”字段内为此配电盘键入可选的简短说明。
6. 如果要自动将此设备上的每个出口添加到“设备”选项卡，则选中“配重所有出口”。
7. 可配置一个类别和元素列表，更好地描述和组织此配电盘以及与其相连的节点。详情参见**第 4 章：创建关联**。
   - 对于每个列出的类别，单击“元素”下拉菜单，然后从列表中选择要应用到设备的元素。对于不想用的类别，从“元素”字段中选择空白项。

   如果看不到要使用的类别或元素值，可通过“关联”菜单进行添加。详情参见**第 4 章：创建关联**。
8. 配置此设备完成后，单击“应用”添加此设备并打开一个空白的“添加设备”屏幕，可继续添加设备。或者，单击“确定”添加此配电盘而不继续显示新的“添加设备”屏幕。

发现设备

“发现设备”可在网络中发起对所有设备的搜索。搜索可自动检测网络上所有新的和以前已经存在的 Raritan 设备，包括 Paragon II System Controller、IP-Reach、Dominion KX、Dominion KX101、Dominion KSX、Dominion SX 和 eRIC。发现设备后如果还未被管理，则可将其添加到 CC-SG。

1. 在“设备”菜单中，单击“发现设备”。出现“发现设备”屏幕。

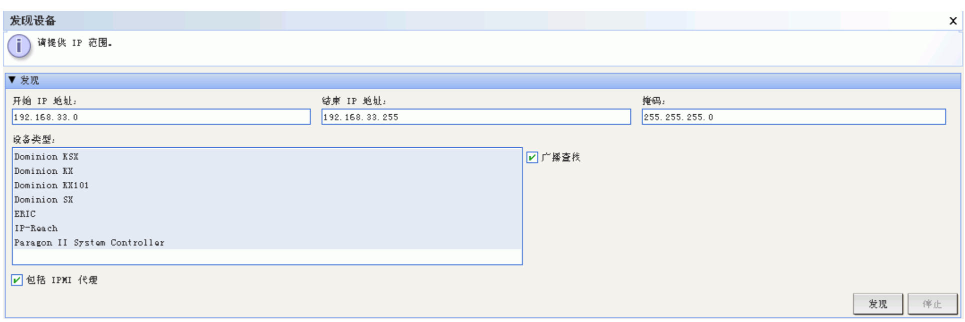


图 32 发现设备屏幕

2. 在“开始地址”和“结束地址”字段中键入需要发现的设备的 IP 地址范围。“结束地址”应大于“开始地址”。指定一个掩码应用到该范围。如果未指定掩码，则会发送广播地址 **255.255.255.255**，将广播到所有本地网络。要发现跨子网的设备，必须指定掩码。
3. 如果在 CC-SG 所在的同一个子网内搜索设备，选中“广播查找”。取消选择“广播查找”即在不同子网内发现设备。
4. 要搜索某个特殊类型的设备，请在“设备类型”列表里选中这种类型。默认情况下，所有设备类型都被选中。按住 **Ctrl** 键单击可选择多个设备类型。
5. 如果要发现提供 IPMI 电源控制的目标，则选中“包括 IPMI 代理”。

6. 单击“发现”开始搜索。在发现过程的任何时候均可单击“停止”停止发现过程。发现的设备显示在一个列表里。

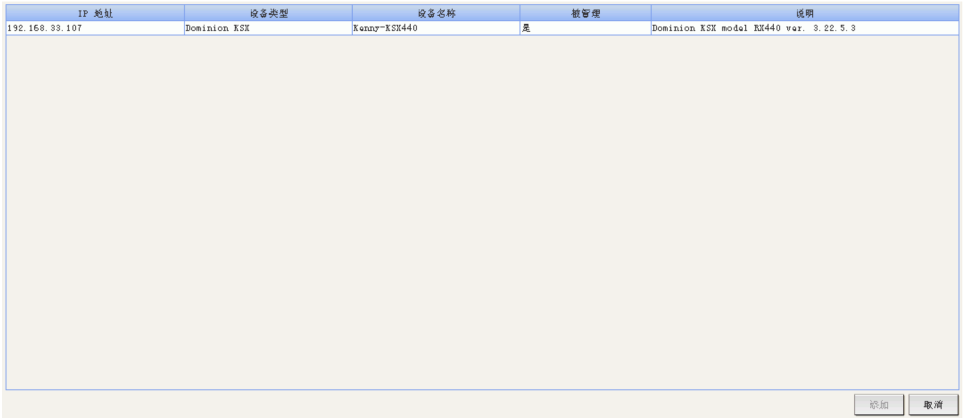


图 33 发现设备列表窗口

7. 要将一个或多个发现的设备添加到 CC-SG，请从列表中选择设备，然后单击“添加”。出现“添加设备”屏幕并填充了一些数据。如果选择多个要添加的设备，可单击屏幕底部的“上一个”和“跳过”在“添加设备”屏幕中导航，查看要添加的设备。

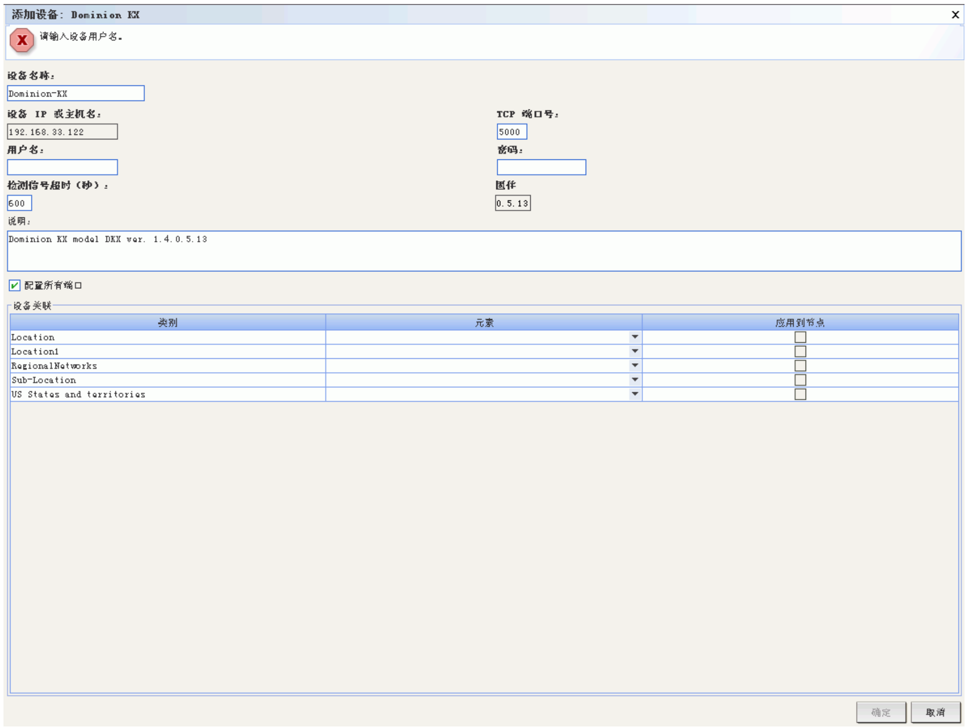


图 34 添加已发现的设备

8. 在“用户名”和“密码”字段内键入用户名和密码（在设备中专门为 CC-SG 创建），即允许 CC-SG 将来与设备通信时对设备进行认证。选择一个“类别”或“元素”应用到该设备。如果要将类别和元素应用到设备上所连的节点，则选中相应的“应用到节点”复选框。

9. 可以根据需要编辑“设备名称”、“检测信号超时”、“本地访问”（如果该设备类型可用）、“说明”、“配置所有端口”和“设备关联”字段。

10. 配置此设备完成后，单击“应用”添加此设备并打开“添加设备”屏幕，可继续添加下一个已发现的设备。或者，单击“确定”添加此设备而不再添加其它已发现的设备。
11. 如果设备的固件版本与 CC-SG 不兼容，将出现警告消息询问是否继续。单击“是”将设备添加到 CC-SG，或单击“否”取消操作。将设备添加到 CC-SG 以后可升级设备固件。详情参阅本章后面的“升级设备”部分。

编辑设备

可对设备进行编辑以重新命名或修改其属性。

1. 单击“设备”选项卡并选择要编辑的设备。出现“设备配置文件”屏幕。

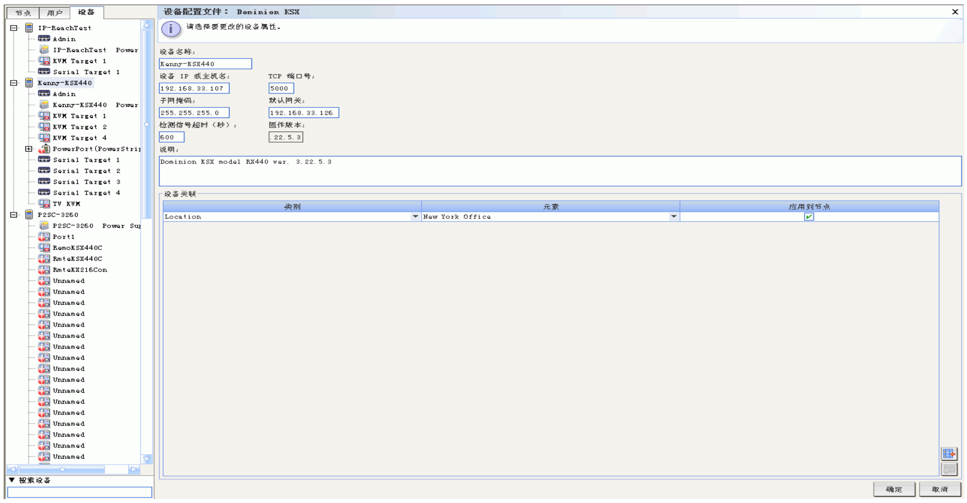


图 35 设备配置文件屏幕

2. 在此屏幕上的合适字段内键入新的设备属性。如果需要，编辑与此设备关联的类别和元素。
3. 单击“确定”保存更改。出现“设备已成功更新”消息即确认设备已被修改。

编辑 PowerStrip 设备

可对受到管理的 PowerStrip 设备进行编辑以重新命名、修改属性或查看出口配置状态。

1. 单击“设备”选项卡并选择要编辑的 PowerStrip 设备。出现“设备配置文件：PowerStrip”屏幕。
2. 在此屏幕上的合适字段内键入新的设备属性。如果需要，编辑与此设备关联的类别和元素。
3. 单击“出口”选项卡查看此 PowerStrip 的所有出口。
   - 如果某个出口与某个节点关联，单击“节点”超链接可打开“节点配置文件”。
   - 如果某个出口与某个节点关联，可选择该出口，然后单击“电源控制”即打开该关联节点的“电源控制”屏幕。
4. 单击“确定”保存更改。出现“设备已成功更新”消息即确认设备已被修改。

删除设备

可删除设备，将其从 CC-SG 管理中去除。

重要说明：删除设备将会删除为其配置的所有端口。与这些端口关联的所有接口也会从该节点删除。如果这些节点不存在其它接口，则节点也会从 CC-SG 中删除。

1. 单击“设备”选项卡并选择要删除的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“删除设备”。出现“删除设备”屏幕。

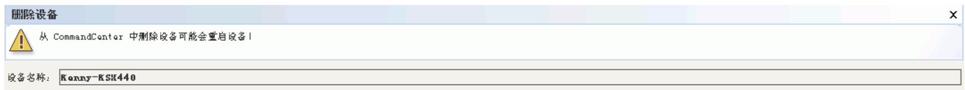


图 36 删除设备屏幕

3. 单击“确定”删除设备，或单击“取消”不删除退出。出现“设备已成功删除”消息即确认设备已被删除。

注：必须先暂停 KSX 设备才可从 CC-SG 中成功删除。要暂停 KSX 设备，在“设备”选项卡中右键单击该设备，然后单击“暂停管理”。在出现的确认消息中单击“是”。KSX 设备将会重新启动。设备暂停后，即可从 CC-SG 中删除。

配置端口

如果设备的端口没有全部自动添加（在“添加设备”屏幕中添加设备时选中“配置所有端口”），则可以使用“配置端口”屏幕将设备上的单个端口或多个端口添加到 CC-SG。必须先配置端口，然后使用这些端口的带外接口才能添加到节点上。

配置串口

1. 单击“设备”选项卡并从设备树中选择一个串行设备。
2. 在“设备”菜单中，单击“端口管理器”，然后单击“配置端口”。出现“配置端口”屏幕。

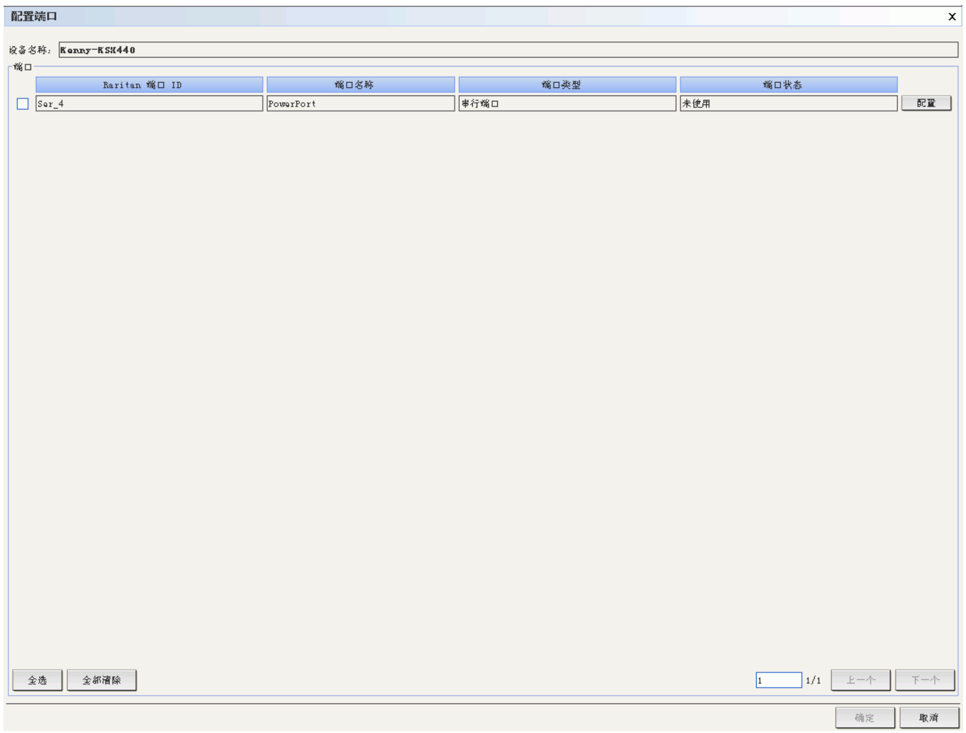


图 37 配置端口屏幕

- 单击一个栏标题即按该属性以升序排列端口。再次单击该标题即按降序排列端口。

3. 单击待配置串口所对应的“配置”按钮。出现“配置串口”屏幕。

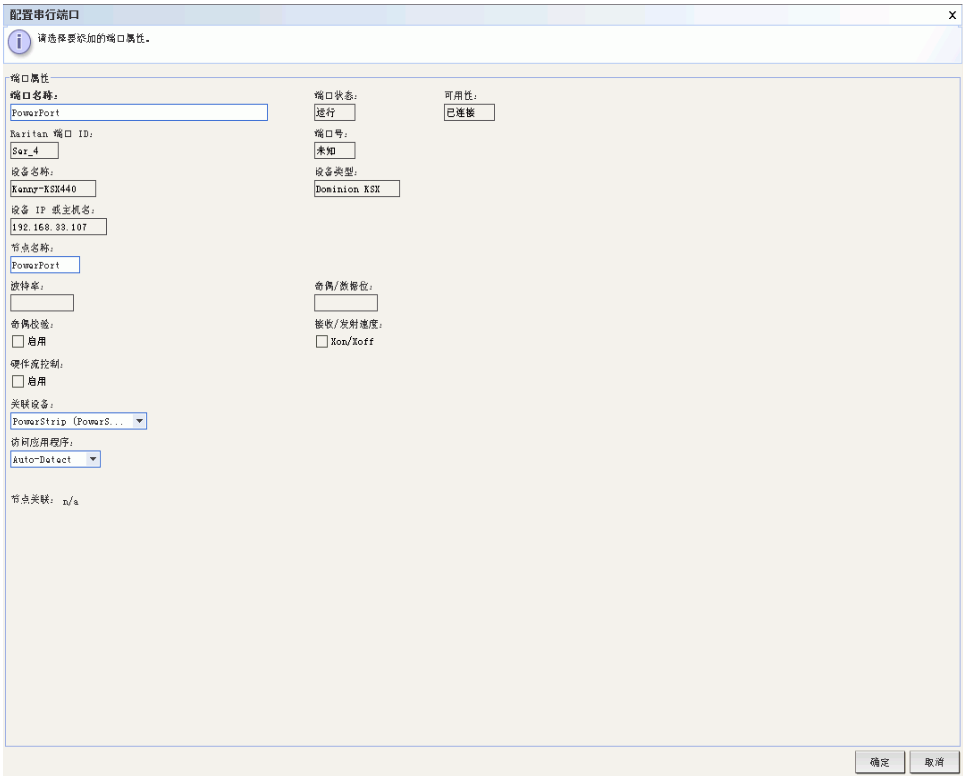


图 38 配置串口屏幕

4. 在“端口名称”字段内键入端口名称。为了使用方便，以端口相连目标的名称开头来命名端口。
5. 在“节点名称”字段中键入节点名称，使用此端口中的一个带外接口创建新节点。为了使用方便，以端口相连目标的名称开头来命名节点。这意味着将在“端口名称”和“节点名称”字段中键入相同的名称。
6. 单击“访问应用程序”下拉菜单，从列表中选择连接此端口时要使用的应用程序。要允许 CC-SG 基于浏览器自动选择正确的应用程序，请选择“自动检测”。
7. 单击“确定”添加端口。

配置 KVM 端口

1. 单击“设备”选项卡并从设备树中选择一个 KVM 设备。
2. 在“设备”菜单中，单击“端口管理器”，然后单击“配置端口”。出现“配置端口”屏幕。

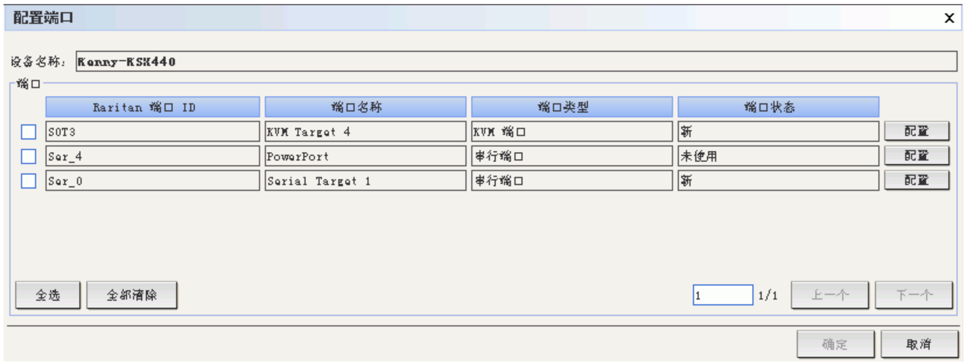


图 39 配置端口屏幕

- 单击一个栏标题即按该属性以升序排列端口。再次单击该标题即按降序排列端口。

3. 单击待配置 KVM 端口所对应的“配置”按钮。出现“配置 KVM 端口”屏幕。

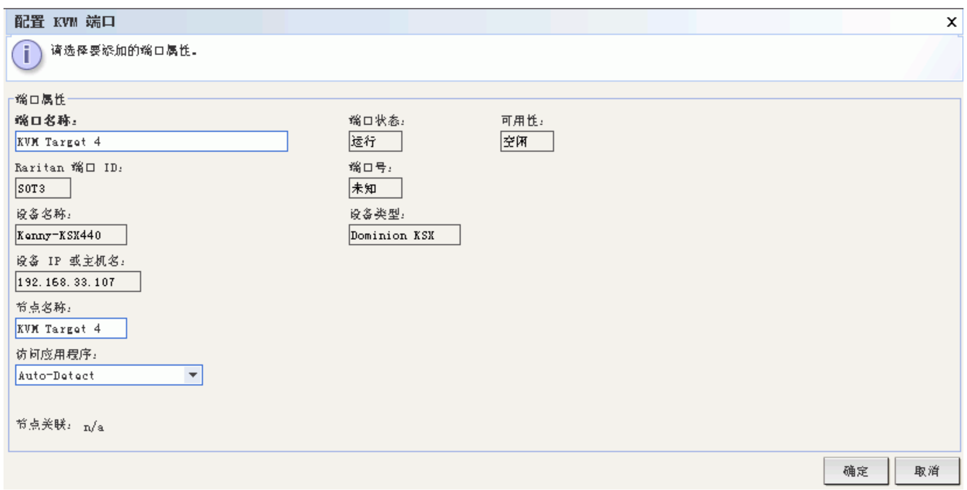


图 40 配置 KVM 端口屏幕

4. 在“端口名称”字段内键入端口名称。为了使用方便，以端口相连目标的名称开头来命名端口。
5. 在“节点名称”字段中键入节点名称，使用此端口中的一个带外接口创建新节点。为了使用方便，以端口相连目标的名称开头来命名节点。这意味着将在“端口名称”和“节点名称”字段中键入相同的名称。
6. 单击“访问应用程序”下拉菜单，从列表中选择连接此端口时要使用的应用程序。要允许 CC-SG 基于浏览器自动选择正确的应用程序，请选择“自动检测”。
7. 单击“确定”添加端口。

编辑端口

可编辑端口以更改名称或者与现有配置端口关联的访问应用程序。

1. 单击“设备”选项卡并选择要编辑的端口。出现“端口配置文件”屏幕。



图 41 端口配置文件

2. 根据需要在“端口名称”字段内键入新的端口名称。
3. 单击“访问应用程序”下拉菜单，从列表中选择连接此端口时要使用的应用程序。要允许 CC-SG 基于浏览器自动选择正确的应用程序，请选择“自动检测”。
4. 单击“确定”保存对已配置端口的更改。

删除端口

删除端口即从设备删除端口条目。

重要说明：如果删除与节点关联的端口，则端口所提供的关联带外 KVM 或串行接口将从节点中删除。如果节点没有其它接口，则节点也会从 CC-SG 中删除。

1. 单击“设备”选项卡并选择要删除端口的设备。
2. 在“设备”菜单中，单击“端口管理器”，然后单击“删除端口”。出现“删除端口”屏幕。

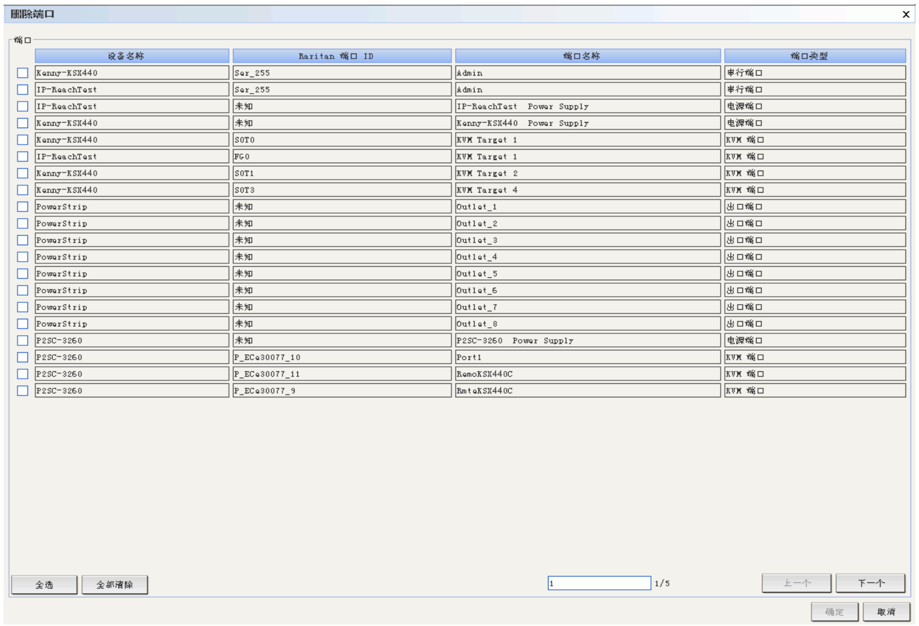


图 42 删除端口屏幕

3. 选中要从设备中删除的端口。
4. 单击“确定”删除所选的端口。出现“端口已成功删除”窗口即确认端口已经删除。

设备管理

设备一旦添加到 CC-SG 以后，除了配置端口以外还可执行几种管理功能。

设备类别和元素的批量复制

“批量复制”命令允许将所分配的类别和元素从一个设备复制到多个其它设备。请注意，此过程中所复制的属性仅仅是类别和元素。

1. 单击“设备”选项卡并从设备树中选择一个设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“批量复制”。出现“批量复制”屏幕。
3. 在“所有设备”列表中，在“设备名称”字段中选择要将设备类别和元素复制到哪些设备。
4. 单击 > 将设备添加“选定设备”列表。
5. 要从“选定设备”列表删除设备，请选择该设备并单击 <。
6. 单击“确定”批量复制，或单击“取消”不复制退出。出现“设备已成功复制”消息即确认该设备类别和元素已被复制。

升级设备

“升级设备”允许下载设备固件的新版本。

1. 单击“设备”选项卡并从设备树中选择一个设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“升级设备”。出现“升级设备”屏幕。

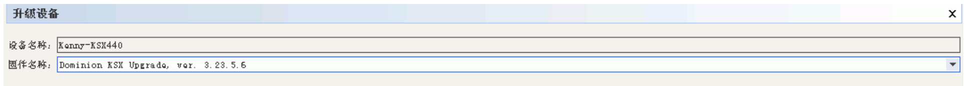


图 43 升级设备屏幕

3. 单击“固件名称”下拉箭头，从列表中选择合适的固件。Raritan 或销售商会提供此信息。单击“确定”升级设备。SX 和 KX 设备的升级需要大约 20 分钟。

   如果设备的固件版本与 CC-SG 不兼容，将出现警告消息询问是否继续。详情参见**第二章：访问 CC-SG**。单击“是”升级设备。

5. 出现“重新启动”消息。单击“是”重新启动设备。
6. 出现“设备已成功升级”消息即确认设备已被升级。

备份设备配置

可为所选的设备备份所有用户配置和系统配置文件。如果设备出现问题，可使用创建的备份文件从 CC-SG 中恢复以前的配置。

1. 单击“设备”选项卡并选择要备份的设备。
2. 在“设备”菜单中，单击“设备管理器”，“配置”，然后单击“备份”。出现“备份设备配置”屏幕。

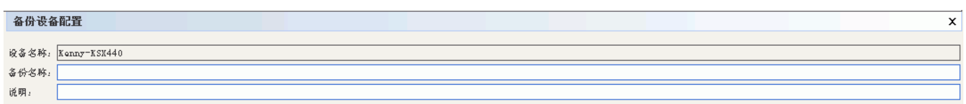


图 44 备份设备配置屏幕

3. 在“备份名称”字段中键入名称来标识此备份。
4. 在“说明”字段内为此备份键入可选的简短说明。
5. 单击“确定”备份设备配置。出现“设备配置已成功备份”消息即确认设备配置已备份。

恢复设备配置

可将以前备份的设备配置恢复到设备。

1. 单击“设备”选项卡并选择要恢复备份配置的设备。
2. 在“设备”菜单中，单击“设备管理器”，“配置”，然后单击“恢复”。出现“恢复设备配置”屏幕。

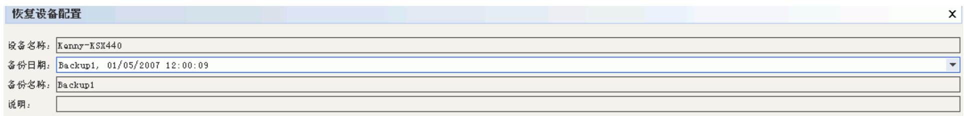


图 45 恢复设备配置屏幕

3. 单击“备份日期”下拉箭头，从列表中选择最后备份设备的日期。备份的名称和说明将会填充在各自的字段中。
4. 单击“确定”恢复备份。
5. 出现“重新启动”消息时，单击“是”重新启动设备。出现“设备配置已成功恢复”消息即确认所有用户和系统配置数据已经恢复。

复制设备配置

此命令允许从一个设备向另一个或多个设备复制配置。

注：只能在具有相同端口号的 Dominion SX 设备之间复制配置。

1. 单击“设备”选项卡，并从设备树中选择一个设备，以将其配置复制到其它设备。
2. 在“设备”菜单中，单击“设备管理器”，“配置”，然后单击“复制配置”。出现“复制设备配置”屏幕。
3. 如果在此设备上曾使用“备份设备”选项，则可选择“从保存的配置”然后从保存的配置下拉菜单内选择配置，通过此法也能复制该配置。
4. 在“可用设备”栏内选择要复制配置的设备，单击向右的箭头将其移到“复制配置到”栏内。向左的箭头可将选定设备移出“复制配置到”栏。
5. 单击“确认”将配置复制到“复制配置到”栏的设备。
6. 出现“重新启动”消息时，单击“是”重新启动设备。出现“设备配置已成功复制”消息即确认设备配置已被复制。

重启设备

“重启设备”命令用于重新启动设备。

1. 单击“设备”选项卡并选择要重启的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“重启设备”。出现“重新启动设备”屏幕。

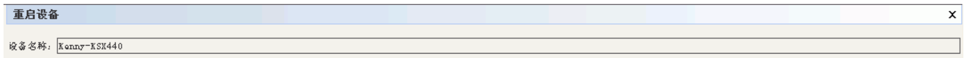


图 46 重启设备屏幕

3. 单击“确定”重新启动设备。出现“设备已成功重新启动”消息即确认设备已重新启动。

Ping 设备

可通过 ping 设备来确定该设备在网络中是否可用。

1. 单击“设备”选项卡并选择要 ping 的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“Ping 设备”。出现“Ping 设备”屏幕，显示 Ping 的结果。

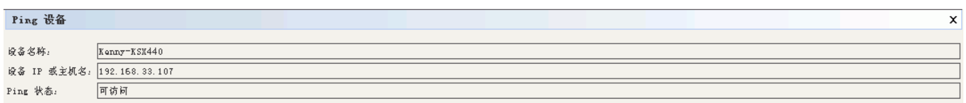


图 47 Ping 设备屏幕

暂停管理

可暂停设备来暂时停止它的 CC-SG 控制，而 CC-SG 内存储的配置数据不会丢失。

1. 单击“设备”选项卡并选择要暂停 CC-SG 管理的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“暂停管理”。设备树内的设备图标将会指示设备的暂停状态。

恢复管理

对于暂停的设备，可恢复其 CC-SG 管理使其重新受到 CC-SG 的控制。

1. 单击“设备”选项卡并从设备树中选择已暂停的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“恢复管理”。设备树内的设备图标将会指示设备的活动状态。

设备电源管理器

设备电源管理器用于查看 PowerStrip 设备的状态（包括电压、电流和温度），并管理 PowerStrip 设备上所有的电源出口。与单独打开和关闭节点电源不同，设备电源管理器提供了以 PowerStrip 为中心的出口视图。

在使用设备电源管理器之前，需要先完成 PowerStrip 与 Dominion SX 或 Dominion KSX 设备之间的物理连接。添加 PowerStrip 设备时，必须定义哪一个 Raritan 设备在提供连接。这会将其关联到 Dominion SX 串口，或者关联到正在提供 PowerStrip 管理的 Dominion KSX 专用电源接口。

1. 在设备树内，选择 PowerStrip 设备。
2. 在“设备”菜单中，单击“设备电源管理器”。出现“设备电源管理器”屏幕。
3. “出口状态”面板中将列出出口。可能需要滚动查看所有出口。
4. 单击每个出口的“开”或“关”单选按钮即打开或关闭出口。
5. 单击“循环”重启与出口连接的设备。
6. 单击“关闭”关闭“设备电源管理器”屏幕。

启动管理

如果可用，“启动管理”命令将提供对所选设备管理员界面的访问。

1. 单击“设备”选项卡，选择要启动管理员界面的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“启动管理”。出现所选设备的管理员界面。

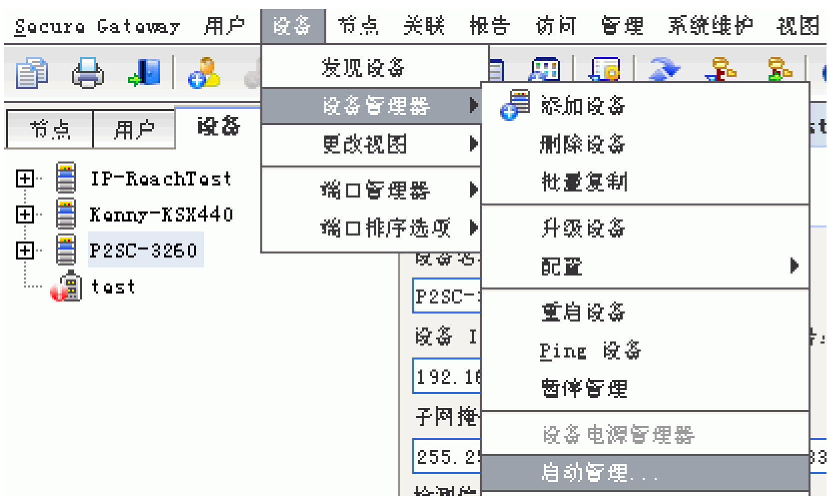


图 48 启动 KX 设备的管理

拓扑视图

拓扑视图显示在配置中所有连接设备的结构化设置。

1. 单击“设备”选项卡，选择要查看拓扑视图的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“拓扑视图”。出现所选设备的“拓扑视图”。

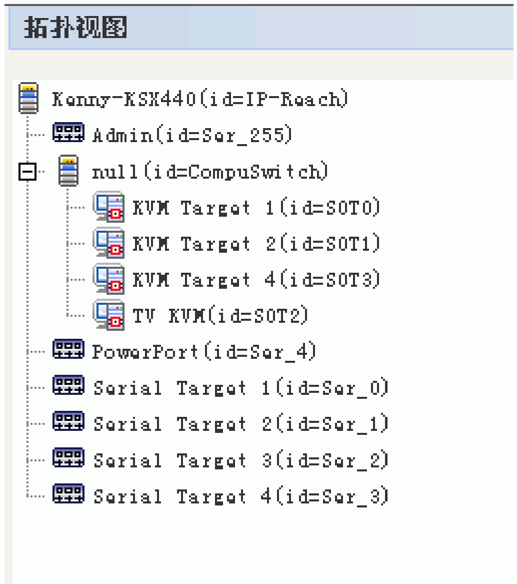


图 49 拓扑视图

3. 在拓扑视图中导航，就像在设备树中一样操作。单击 + 和 - 符号即展开和收缩视图。
4. 单击“关闭”关闭“拓扑视图”屏幕。

*注：在**关闭拓扑视图**之前，这个视图将会代替选择设备时正常出现的“设备配置文件”屏幕。*

断开用户连接

管理员可终止任何用户与设备的会话。包括正在设备上执行任何类型操作的用户，如连接端口、备份设备配置、恢复设备配置或升级设备固件。

注：对于固件升级与设备配置备份和恢复，可在操作完成后再终止用户与设备的会话。所有其它操作将会立即终止。

1. 单击“设备”选项卡，选择要断开一个或多个用户连接的设备。
2. 在“设备”菜单中，单击“设备管理器”，然后单击“断开用户连接”。出现“断开用户连接”屏幕。

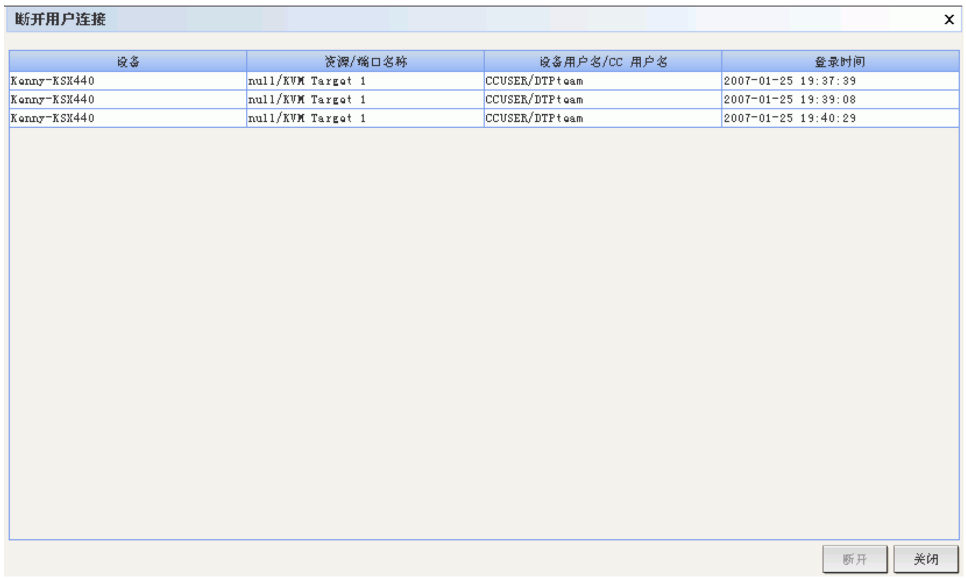


图 50 断开用户连接

3. 在“断开用户连接”表内选择要断开会话的用户。
4. 单击“断开连接”从设备上断开其连接。

注：仅对于 Dominion SX 设备，可断开直接登录到设备的用户以及通过 CC-SG 连接到设备的用户。

查看设备

CC-SG 提供不同的选项在“设备”选项卡中显示设备。

树形视图

选择“树形视图”即在默认视图组织的设备树中查看设备。选择“树形视图”将会从“自定义视图”返回到标准视图。详情参阅本章后面的“自定义视图”部分。

1. 在“设备”菜单中，单击“更改视图”，然后单击“树形视图”。出现设备的标准“树形视图”。

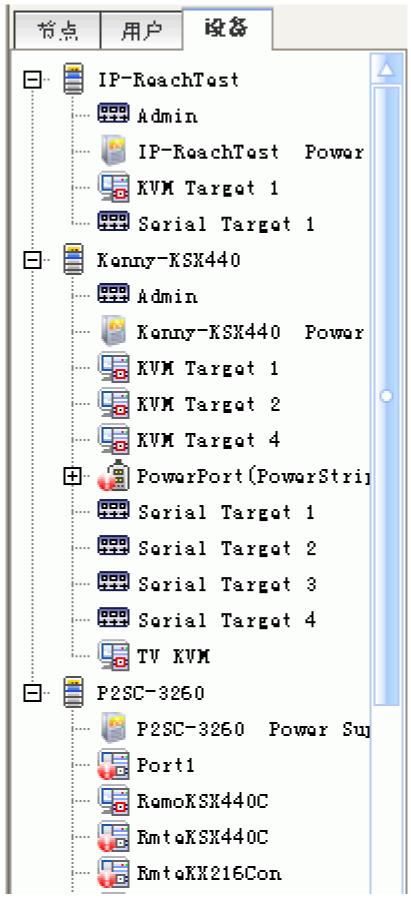


图 51 设备树普通视图屏幕

已配置的端口内嵌于父设备下面。要更改端口显示的方式，请单击“设备”菜单，然后单击“端口排序选项”。选择“按端口名称”或“按端口状态”即按照名称的字母顺序或按照可用性状态排列其设备内的端口。按状态排列的端口在其连接状态分组内按照字母顺序排序。设备也会相应地进行排序。

自定义视图

可通过自定义设备树以特殊格式组织所显示的设备。可按国家、时区或有助于区分它们的其它选项来查看设备。有关向 CC-SG 添加类别的详细信息，请参阅**第 4 章：创建关联**。

1. 单击“设备”选项卡。
2. 在“设备”菜单中，单击“更改视图”，然后单击“创建自定义视图”。出现“自定义视图”屏幕。

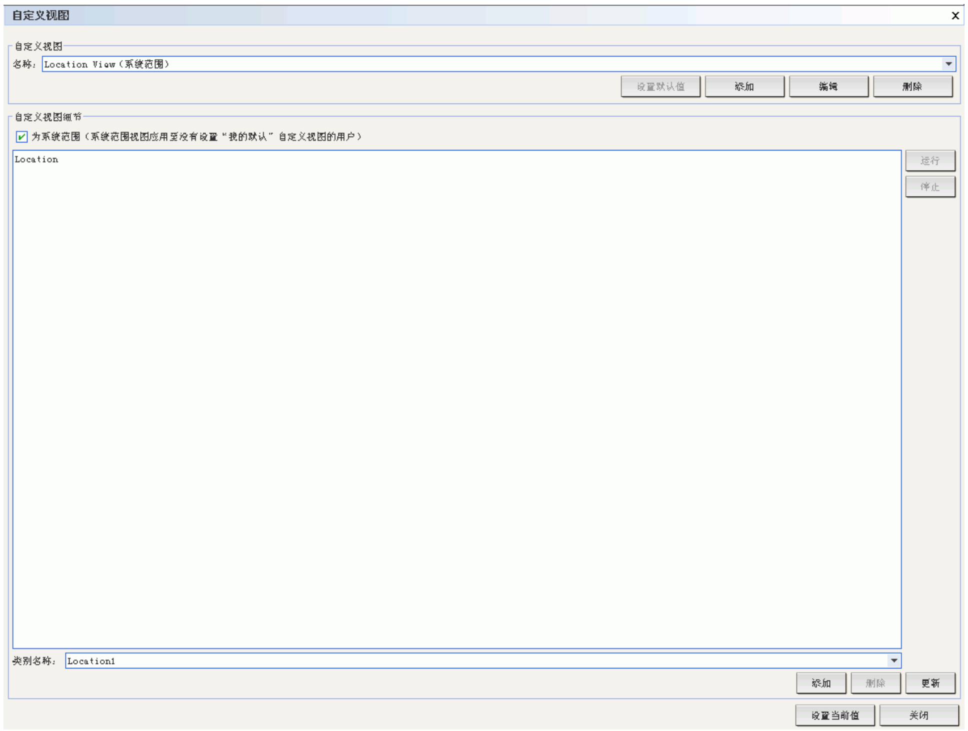


图 52 自定义视图屏幕

3. 要自定义视图，请单击“名称”下拉箭头，选择数据库中已经保存的自定义视图。视图类别的详细信息显示在“自定义视图细节”字段内。
4. 单击“设置当前值”即按所选的自定义视图排列设备树。
5. 如果想要在登录 CC-SG 后即显示所选的自定义视图，请单击“设置默认值”。
6. 选中“为系统范围”将其作为所有不使用自己自定义视图的用户的默认视图。

选择自定义视图

要将当前的“设备树”视图快速更改为已经建立的自定义视图：

1. 单击“设备”选项卡。
2. 在“设备”菜单中，单击“更改视图”，然后选择在“创建自定义视图”下面列出的自定义视图名称。设备树将变成所选的自定义视图。

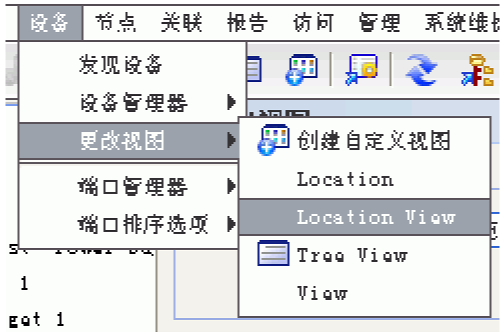


图 53 选择自定义视图

添加自定义视图

1. 单击“设备”选项卡。
2. 在“设备”菜单中，单击“更改视图”，然后单击“创建自定义视图”。出现“自定义视图”屏幕。
3. 在“自定义视图”面板内，单击“添加”。出现“添加自定义视图”窗口。
4. 键入新的自定义视图名称，然后单击“确定”，或单击“取消”关闭窗口。在“名称”字段内出现新视图的名称。
5. 在“自定义视图细节”面板内，单击面板底部的下拉箭头。此列表中包含的类别可用于过滤自定义视图。从下拉列表内选择一个细节，然后单击“添加”将该细节添加到“自定义视图细节”面板内。根据需要选择多个细节。
6. 要对“自定义视图细节”面板内的细节重新排列顺序，请选择一个细节并按“向上”或“向下”按钮，即可按设备排列的顺序排列细节。要从列表中删除细节，请选择该细节并单击“自定义视图细节”面板内的“删除”按钮。
7. 单击“更新”即更新自定义视图。出现“自定义视图已成功更新”消息即确认自定义视图已经更新。
8. 单击“设置当前值”即按所选的自定义视图排列设备树。

编辑自定义视图

1. 单击“设备”选项卡。
2. 在“设备”菜单中，单击“更改视图”，然后单击“自定义视图”。出现“自定义视图”屏幕。
3. 在“自定义视图”面板内单击“名称”下拉箭头，选择要编辑的自定义视图。单击“编辑”。出现“编辑自定义视图”窗口。
4. 键入新的自定义视图名称，然后单击“确定”确认，或单击“取消”关闭窗口。
5. 在“自定义视图细节”面板内，单击面板底部的下拉箭头。此列表中包含的类别可用于过滤自定义视图。从下拉列表内选择一个细节，然后单击“添加”将该细节添加到“自定义视图细节”面板内。根据需要选择多个细节。

6. 要对“自定义视图细节”面板内的细节重新排列顺序，请选择一个细节并按“向上”或“向下”按钮，即可按设备排列的顺序排列细节。要从列表中删除细节，请选择该细节并单击“自定义视图细节”面板内的“删除”按钮。
7. 单击“更新”即更新自定义视图。出现“自定义视图已成功更新”消息即确认自定义视图已经更新。
8. 单击“设置当前值”即按所选的自定义视图排列设备树。

删除自定义视图

1. 单击“设备”选项卡。
2. 在“设备”菜单中，单击“更改视图”，然后单击“创建自定义视图”。出现“自定义视图”屏幕。

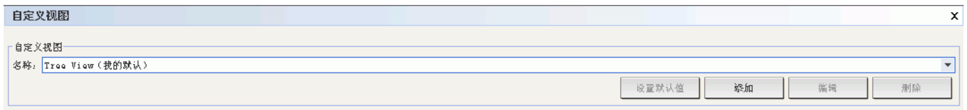


图 54 自定义视图屏幕

3. 在“自定义视图”面板内单击“名称”下拉箭头，选择要删除的自定义视图。
4. 在“自定义视图”面板内单击“删除”按钮。出现“删除自定义视图”窗口。
5. 单击“是”删除该自定义视图。

特别访问 Paragon II 系统设备

Paragon II System Controller (P2-SC)

Paragon II System Integration 用户可将其 P2-SC 设备添加到 CC-SG 设备树中，并通过 CC-SG 内的 P2-SC Admin 应用程序对其进行配置。有关 P2-SC Admin 使用的详细信息，请参阅 Raritan 的《Paragon II System Controller 用户指南》。

将 Paragon System 设备（Paragon System 包括 P2-SC 设备、连接的 UMT 设备和连接的 IP-Reach 设备）添加到 CC-SG 以后，即会出现在设备树内。

要访问 Paragon II System Controller：

1. 单击“设备”选项卡，然后选择“Paragon II System Controller”。
2. 右键单击 Paragon II System Controller，然后单击“启动管理”在新的浏览器窗口中启动 Paragon II System Controller 应用程序。然后可配置 PII UMT 设备。

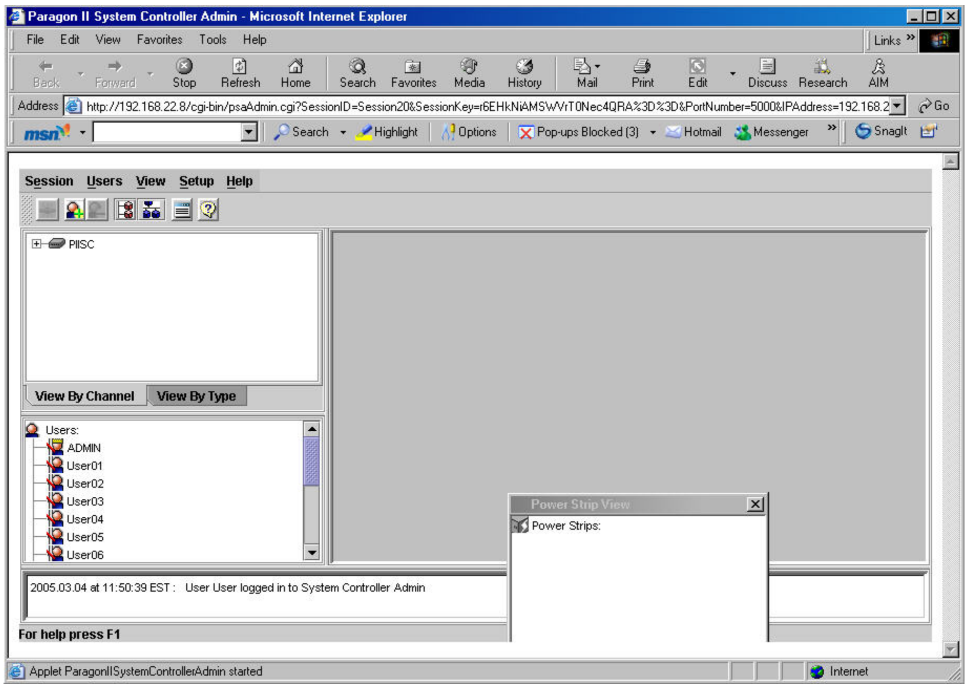


图 55 Paragon 管理器应用程序窗口

IP-Reach 和 UST-IP 管理

也可直接从 CC-SG 界面上对 Paragon System 上连接的 IP-Reach 和 UST-IP 设备执行管理诊断。

将 Paragon System 设备添加到 CC-SG 以后，即会出现在设备树内。

要访问远程用户工作站管理：

1. 单击“设备”选项卡，然后选择“Paragon II System Controller”。
2. 右键单击“Paragon II System Controller”，然后单击“远程用户工作站管理”。出现“远程用户工作站管理”屏幕，列出所有连接的 IP-Reach 和 UST-IP 设备。
3. 在要操作的设备行内单击“启动管理”按钮，即可激活 Raritan 远程控制台并在新窗口内启动蓝色的设备配置屏幕。

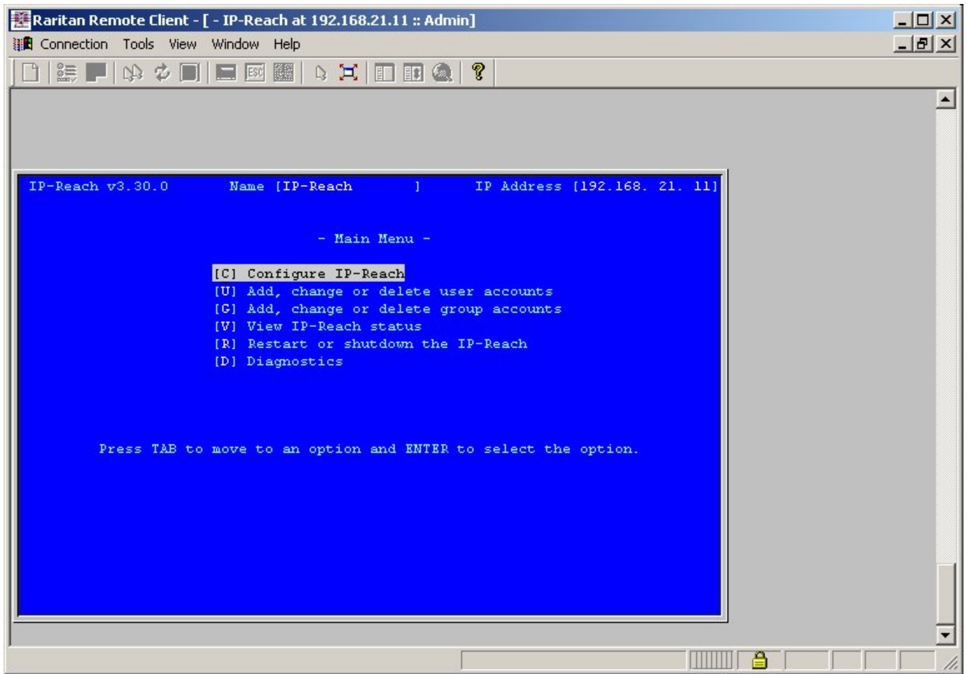


图 56 IP-Reach 管理屏幕

设备组管理器

“设备组管理器”屏幕可用来添加、编辑和删除设备组。添加新的设备组时，可为该组创建完整访问策略。详情参见**第 8 章：策略**。

添加设备组

1. 在“关联”菜单中，单击“设备组”。打开“设备组管理器”窗口。左侧面板内显示现有的设备组。

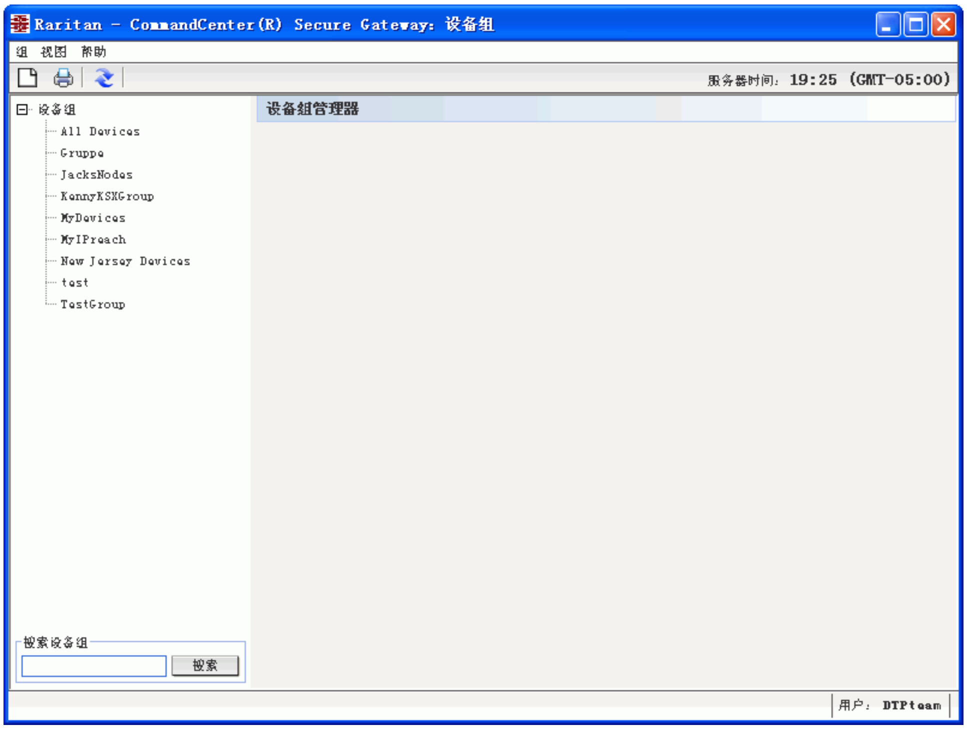


图 57 设备组管理器

2. 单击工具栏内的新建组图标 。显示“设备组：新建”面板。

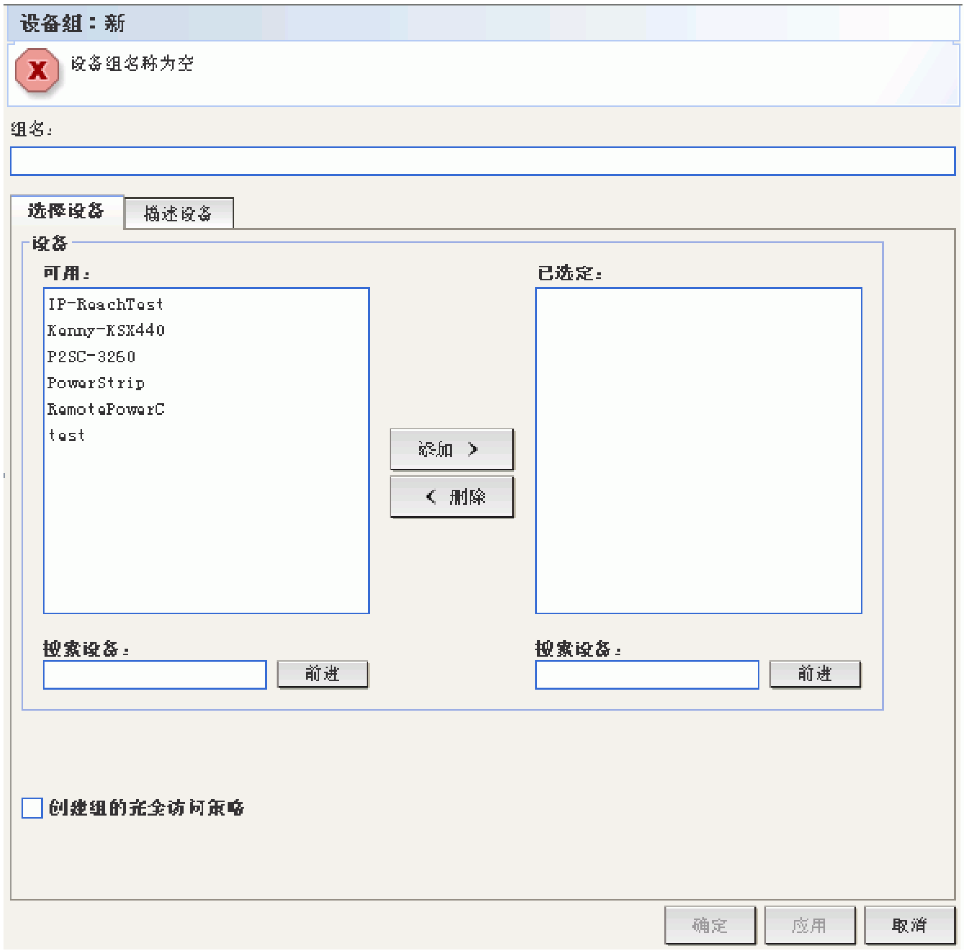


图 58 设备组：新建面板，选择设备选项卡

3. 在“组名称”字段中，为要创建的设备组键入名称。
4. 将设备添加到组可通过两种方式：“选择设备”和“描述设备”。“选择设备”选项卡允许通过从可用设备列表中选择设备，从而选择将哪些设备指定给组。“描述设备”选项卡允许指定描述设备的规则，参数符合这些规则的设备将被添加到组中。

选择设备

a. 在“添加设备组”面板内单击“设备组：新建”选项卡。

b. 在“可用”列表中选择要添加到组中的设备，然后单击“添加”将设备移到“已选定”列表中。“已选定”列表中的设备将被添加到组中。

- 如果需要从组中删除某个设备，请从“已选定”列表选择该设备名称，然后单击“删除”。
- 可在“可用”或“已选定”列表中搜索设备。在列表下面的字段中键入搜索术语，然后单击“执行”。

描述设备

a. 在“描述设备组”面板内单击“设备组：新建”选项卡。在“描述设备”选项卡中，可创建一个规则表来描述要指定到组中的设备。

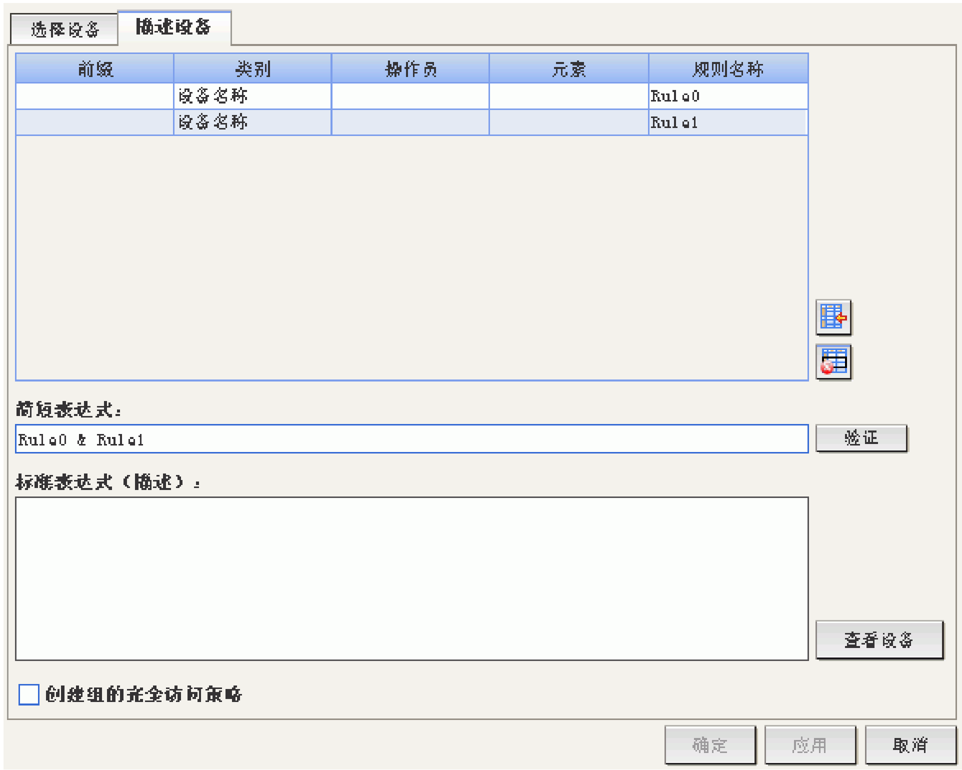


图 59 描述设备选项卡

b. 单击添加新行图标  向表中添加一行。

c. 双击为每列创建的单元格激活下拉菜单。选择要从每个列表中使用的规则组件。

- **前缀**——留空或选择“否”。如果选择“否”，此规则将过滤与表达式其他相反的值。
- **类别**——选择规则中将要评估的一种属性。此处将提供在“关联管理器”中创建的所有类别。
- **运算符**——选择一种在类别和元素项之间要执行的比较运算。提供三种运算符：=（等于）、**LIKE**（用于在名称中发现元素）以及 <>（不等于）。
- **元素**——为要比较的类别属性选择一个值。只有与所选类别关联的元素会在此显示（例如：如果评估“部门”类别，则“Location”元素不会在此出现）。
- **规则名称**——指定给此行内规则的名称。不可编辑，用于在“简短表达式”字段中写入说明。

例如规则 `Department = Engineering` 表示描述类别“Department”设为“Engineering”的所有设备。这与在“添加设备”操作中配置关联时的情形完全一样。

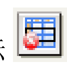
d. 如果要添加其它规则，单击“添加新行”，然后进行必要的配置。配置多个规则可提供多个评估设备的标准，从而进行更为精确的描述。

e. 规则表仅将标准用于评估节点。要为设备组编写描述，请在“简短表达式”字段中按“规则名称”添加规则。如果描述仅需要一个简单的规则，则只需简单地在字段中键入规则名称即可。如果要评估多个规则，请将规则键入字段中，并使用逻辑运算符集描述规则之间的关系。

- **&** – “与”运算符。节点必须满足此运算符两侧的规则，描述（或该描述部分）才被评估为真。
- **|** – “或”运算符。设备仅需满足此运算符两侧的任一规则，描述（或该描述部分）才被评估为真。
- **(** and **)** – 分组运算符。将描述划分为几个部分，用括号包含。首先评估括号内的部分，然后再将描述的其余部分与节点比较。括号对可内嵌于另一括号对内。

例如：要描述隶属于工程部的设备，则创建规则 `Department = Engineering`。这个为 Rule0。然后在“简短表达式”字段中键入 Rule0。

又例如：要描述隶属于工程部或者位于 Philadelphia 的一组设备，并且指定所有设备必须有 1 GB 的内存，则需要开始创建三个规则。`Department = Engineering` (Rule0) `Location = Philadelphia` (Rule1) `Memory = 1GB` (Rule2)。这些规则需要按一定关系排列起来。由于设备可以隶属于工程部或者位于 Philadelphia，因此使用“或”运算符 `|` 连接二者：`Rule0|Rule1`。需要将其放到括号内先进行比较：`(Rule0|Rule1)`。最后，由于设备必须满足此比较结果“并且”要有 1GB 的内存，因此要使用“与”运算符 **&** 将此部分与 Rule2 连接：`(Rule0|Rule1)&Rule2`。然后在“简短表达式”字段中键入这个最终的表达式。

- 如果要从表中删除一行，请选择该行，然后单击删除选定行图标 。
- 如果要查看哪些设备的参数满足所定义的规则，请单击“查看设备”。

f. 将描述写入“简短表达式”后，单击“验证”。如果描述的格式不正确，则会收到一条警告。如果描述的格式正确，则“标准表达式”字段中将会出现此表达式的标准化格式。

g. 单击“查看设备”查看哪些节点满足此表达式。将出现“设备组结果中的设备”窗口，显示将按当前表达式进行分组的设备。这可用于检查表达式是否正确编写。如果不正确，可返回到规则表或“简短表达式”字段进行修改。

h. 要为此设备组创建一个策略允许对组内所有设备在所有时间拥有控制权限访问，则选中“创建组的完全访问策略”。

i. 如果想要添加其它设备组，请单击“应用”保存该组，然后重复本节中的步骤添加其它设备组。如果添加设备组完成，单击“确定”保存此组并退出“设备组：新建”面板。

编辑设备组

1. 在“关联”菜单中，单击“设备组”。打开“设备组管理器”窗口。

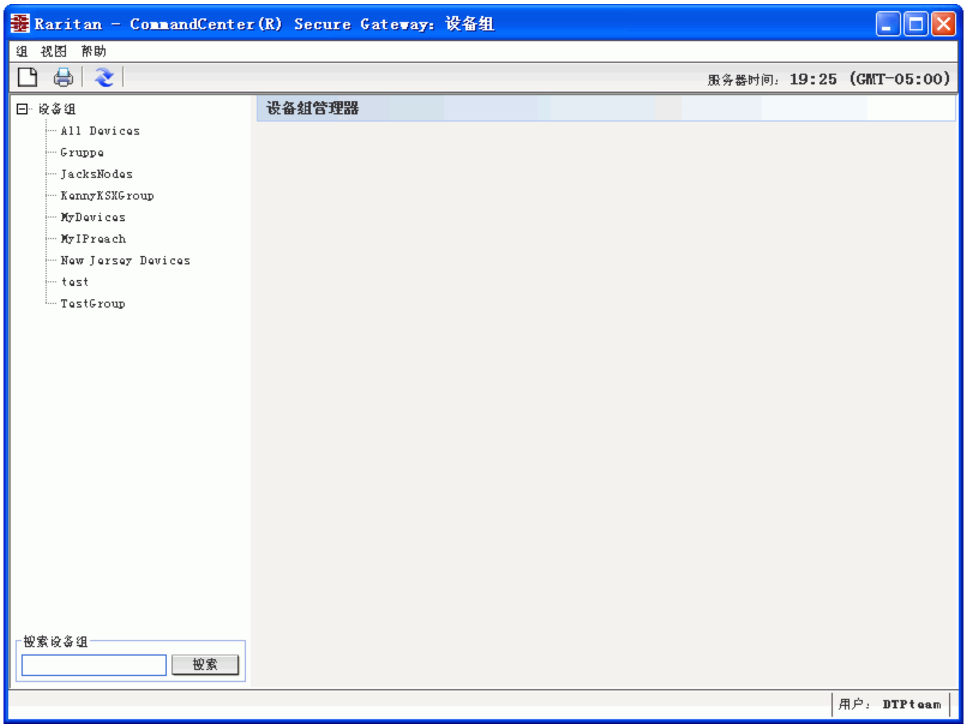


图 60 设备组管理器屏幕

2. 左侧面板内显示现有的设备组。选择要编辑名称的设备组。显示“设备组细节”面板。
3. 如果要编辑设备组名称，请在“组名称”字段内键入设备组的新名称。
4. 使用“选择设备”或“描述设备”选项卡编辑设备组所含的设备。详情参阅上节“添加设备组”。
5. 单击“确定”保存更改。

删除设备组

1. 在“关联”菜单中，单击“设备组”。打开“设备组管理器”窗口。

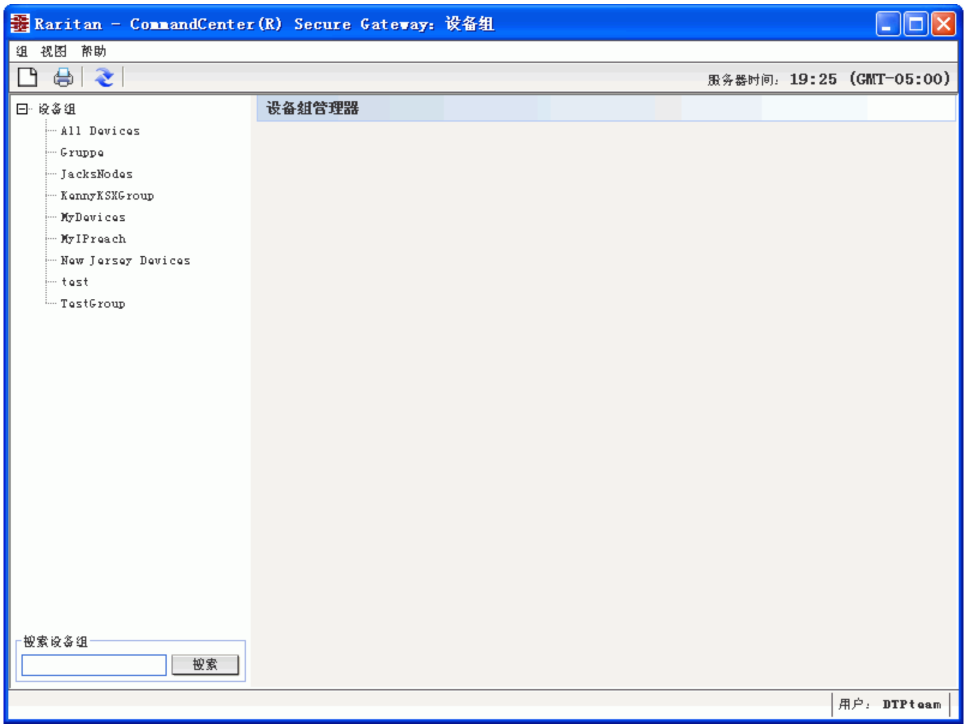


图 61 设备组管理器屏幕

2. 左侧面板内显示现有的设备组。选择要删除的设备组。显示“设备组细节”面板。
3. 在“组”菜单中，单击“删除”。



图 62 删除设备组窗口

4. 显示“删除设备组”面板。单击“删除”。

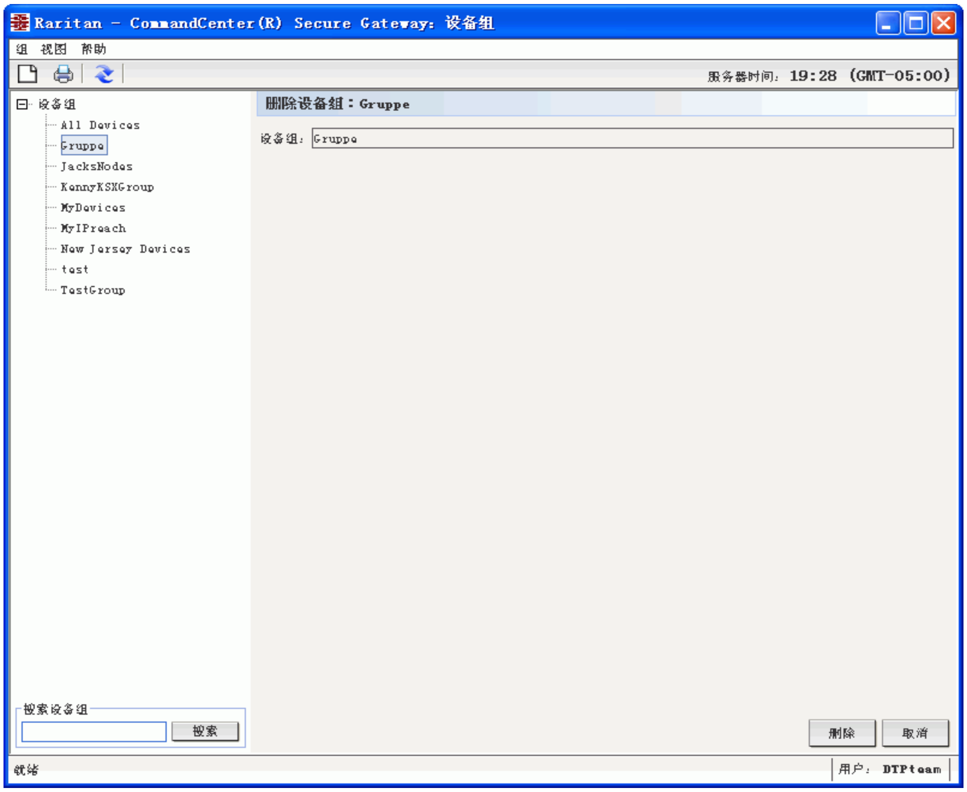


图 63 删除设备组面板

5. 在出现的确认消息中单击“是”。

此页专门留白。

第 6 章：配置节点和接口

本章讨论如何查看、配置和编辑节点及其关联的接口。有关连接节点的详细信息，请参阅 Raritan 的《CommandCenter Secure Gateway 用户指南》。

查看节点

在 CC-SG 内，可在节点树内查看所有节点，并可以选择一个节点查看其节点配置文件。

节点树

单击“节点”选项卡时，“节点”树显示可用的节点。节点按名称的字母顺序排序，或按照可用性状态分组。按可用性状态分组的节点在其可用性分组内按照字母顺序排序。要切换排序方式，请右键单击树，单击“节点排序选项”，然后单击“按节点名称”或“按节点状态”。

节点配置文件

在节点树内单击一个节点打开“节点配置文件”屏幕，内含有关节点、其接口、默认接口、分配到节点的类别和元素的信息。

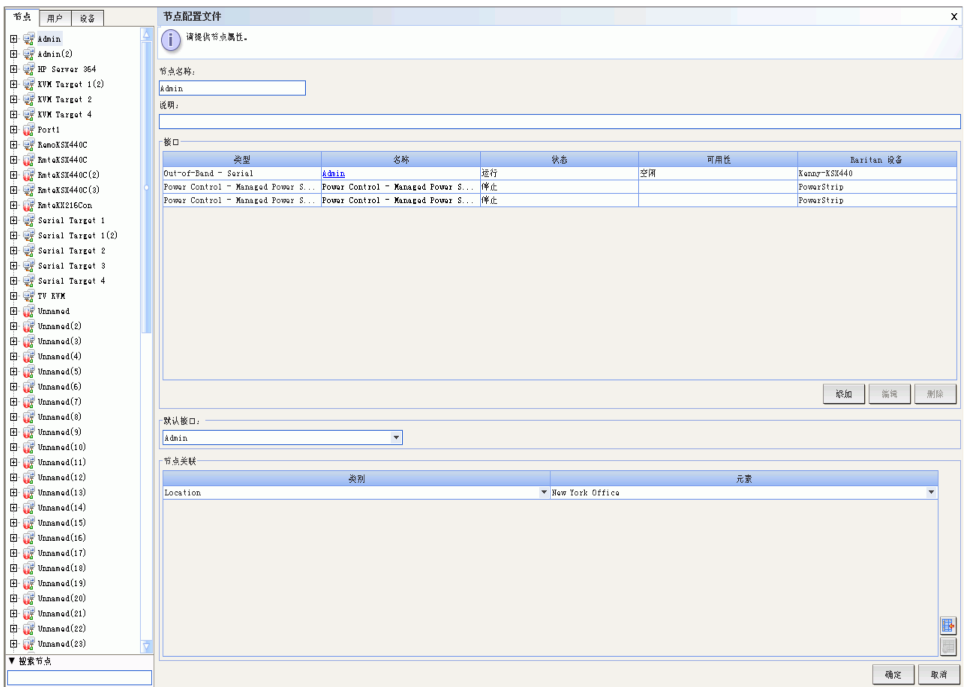


图 64 节点树和节点配置文件屏幕

节点和接口图标

为了便于识别，节点在节点树上有不同的图标。将鼠标指针停留在节点树内的图标上，即可看到有关该节点信息的工具提示。

图标	含义
	节点可用 – 节点至少有一个运行的接口。
	节点不可用 – 节点没有正在运行的接口。

节点和接口概述

关于节点

每个节点代表一个可通过 CC-SG 采用带内（直接 IP）或带外（连接到 Raritan 设备）方法进行访问的目标。例如，节点可以是机架内一台连接 Raritan KVM over IP 设备的服务器、一台带有 HP iLO 卡的服务器、运行 VNC 的网络上的一台 PC 或者一个采用远程串行管理连接的组网基础设施。

添加节点所连的设备以后，即可手动将节点添加到 CC-SG。但是，节点也可以自动创建，即添加设备时在“添加设备”屏幕上选中“配置所有端口”复选框。这种选项允许 CC-SG 自动添加所有设备端口，并为每个端口添加一个节点和一个带外 KVM 或串口。按照本章所述的方法，可在以后随时编辑这些节点、端口和接口。详情参阅**第 3 章：使用指导设置配置 CC-SG** 或**第 5 章：添加设备和设备组中的添加设备**。

节点名称

节点名称必须是唯一的。如果尝试手动添加一个节点使用现有节点名称，CC-SG 将通过选项进行提示。CC-SG 自动添加节点时，编号系统保证节点名称是唯一的。

关于接口

在 CC-SG 内，节点可通过接口访问。必须为每个新节点添加至少一个接口。可为节点添加不同类型的接口以提供不同种类的访问，例如带外 KVM、串行，或者电源控制，或者带内 SSH/RDP/VNC 或 DRAC/RSA/ILO，这取决于节点类型。

单个节点可有多个接口，但只能有一个带外串行或 KVM 接口。例如，运行 Windows Server 2003 的 PC 有一个带外 KVM 接口通过其键盘、鼠标和监视器端口，有一个电源接口来管理所连接的出口。

重要事项！本章介绍的很多菜单栏命令可通过快捷菜单进行访问，即右键单击节点，然后从显示的快捷菜单中选择命令。

添加节点

要将新节点添加到 CC-SG：

1. 单击“节点”选项卡。
2. 在“节点”菜单中，单击“添加节点”。出现“节点配置文件”屏幕。

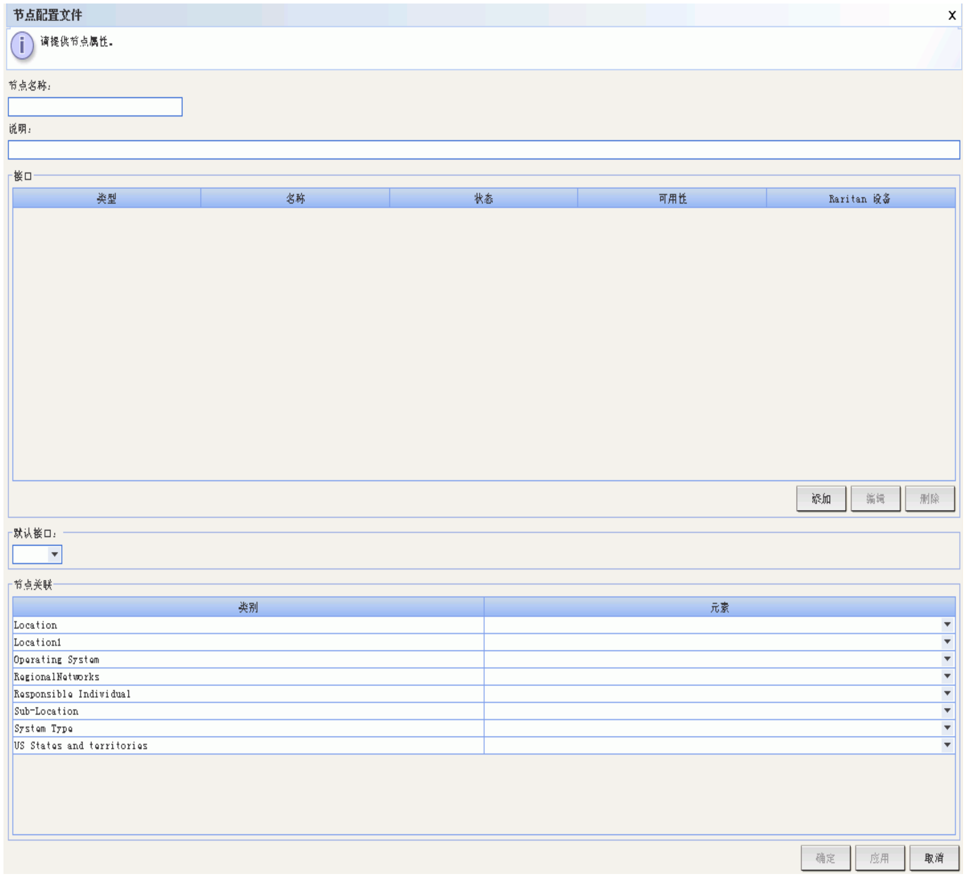


图 65 添加节点屏幕

3. 在“节点名称”字段内键入节点的名称。在 CC-SG 内所有节点名称必须是唯一的。
4. 在“说明”字段内为此节点键入可选的简短说明。
5. 必须配置至少一个接口。在“添加节点”屏幕的“接口”区域内，单击“添加”可添加接口。有关此过程的详细信息，详情参阅“添加接口”部分。
6. 可配置一个类别和元素列表，更好地描述和组织此节点。详情参见第 4 章：创建关联。
   - 对于每个列出的类别，单击“元素”下拉菜单，然后从列表中选择要应用到节点的元素。对于不想用的类别，从“元素”字段中选择空白项。
   - 如果看不到要使用的类别或元素值，可通过“关联”菜单进行添加。详情参见第 4 章：创建关联。
7. 单击“确定”保存节点。节点将被添加到节点列表内。

添加接口

1. 对于现有节点：单击“节点”选项卡，然后选择要添加接口的节点。出现“节点配置文件”屏幕，单击“接口”部分内的“添加”。如果正在添加新节点：在“添加节点”屏幕的“接口”部分内，单击“添加”。出现“添加接口窗口”。
2. 单击“接口类型”下拉菜单，选择节点所用的连接类型：

带内连接

- **DRAC KVM**：选择此项即通过 DRAC 接口创建到 Dell DRAC 服务器的 KVM 连接。此后需要配置一个 DRAC Power 接口。
- **RDP**：选择此项即使用远程桌面协议创建到节点的 KVM 连接，例如 Windows 服务器上的远程桌面连接。
- **RSA KVM**：选择此项即通过 RSA 接口创建到 IBM RSA 服务器的 KVM 连接。此后需要配置一个 RSA Power 接口。
- **SSH**：选择此项即创建到节点的 SSH 连接。
- **VNC**：选择此项即通过 VNC 服务器软件创建到节点的 KVM 连接。
- **iLO/RILOE KVM**：选择此项即通过 iLO 或 RILOE 接口创建到 HP 服务器的 KVM 连接。

带外连接

- **KVM**：选择此项即通过 Raritan KVM 设备（KX、KX101、KSX、IP-Reach、Paragon II）创建到节点的 KVM 连接。
- **串行**：选择此项即通过 Raritan 串行设备（SX、KSX）创建到节点的串行连接。

电源连接

- **DRAC**：选择此项即创建到 Dell DRAC 服务器的电源控制连接。
- **IPMI**：选择此项即通过 IPMI 连接创建到节点的电源控制连接。
- **被管 PowerStrip**：选择此项即通过 Raritan 串行被管的 PowerStrip 创建到节点的电源控制连接。
- **RSA**：选择此项即创建到 RSA 服务器的电源控制连接。
- **iLO/RILOE**：选择此项即创建到 HP iLO/RILOE 服务器的电源控制连接。

3. 根据选择，在“名称”字段中将出现默认名称。可根据需要更改此名称。此名称将出现在节点列表内接口的旁边。

对于带内连接和 DRAC、RSA 以及 iLO/RILOE 电源连接

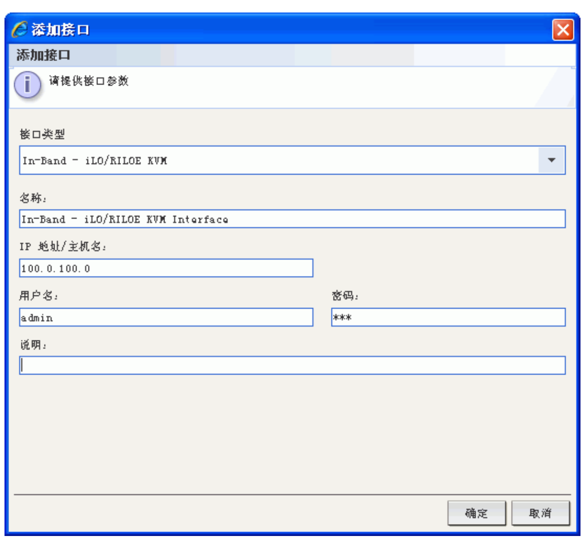


图 66 添加接口—带内 iLO/RILOE KVM

a. 在“IP 地址/主机名”字段中键入此接口的 IP 地址或主机名。
b. 根据需要在“TCP 端口”字段内为此连接键入 TCP 端口。
c. 在“用户名”字段内为此连接键入用户名。
d. 根据需要在“密码”字段内为此连接键入密码。
e. 单击“确定”将接口添加到节点。将返回到“添加节点”或“节点配置文件”屏幕。

对于带外 KVM、带外串行连接：

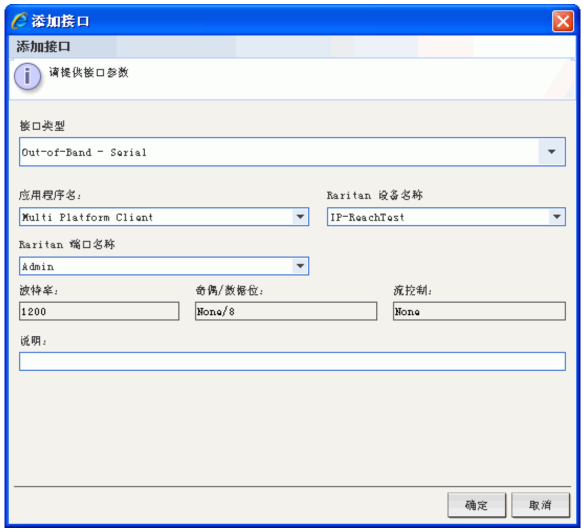


图 67 配置带外 KVM 连接

a. 单击“应用程序名称”下拉菜单，从列表中选择连接此节点时要使用的应用程序。要允许 CC-SG 基于浏览器自动选择应用程序，请选择“自动检测”。
b. 单击“Raritan 设备名称”下拉菜单，选择为节点提供访问 Raritan 的设备。注意，必须首先为 CC-SG 添加一台设备，才会在列表中显示。
c. 单击“Raritan 端口名称”下拉菜单，选择为节点提供访问 Raritan 的设备端口。端口必须先在 CC-SG 内配置后，才会出现在列表内。在串行连接上，“波特率”、“奇偶校验”和“流控”值将根据端口配置填充。
d. 单击“确定”将接口添加到节点。将返回到“添加节点”或“节点配置文件”屏幕。

对于被管配电盘连接

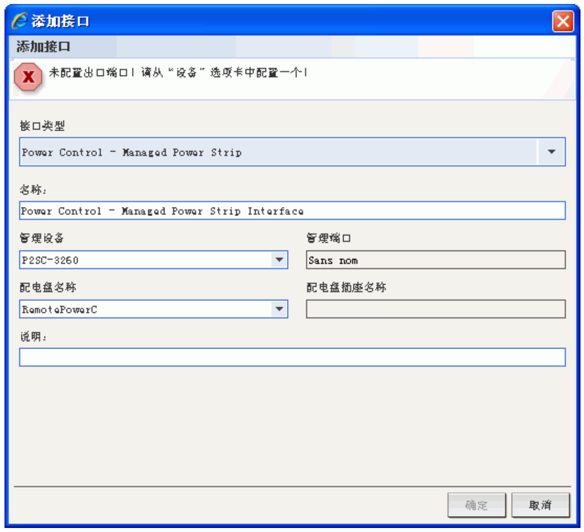


图 68 配置被管配电盘电源控制接口

a. 单击“管理设备”下拉菜单，选择 Raritan 设备用于管理为节点提供电源的配电盘。所选择的设备必须先添加到 CC-SG，才会出现合适的选项。

b. 单击“配电盘名称”下拉菜单，选择为节点提供电源的配电盘。必须首先在 CC-SG 中配置配电盘，才会在列表中显示。

c. 单击“配电盘出口名称”，选择节点所插入的电源出口名称。

d. 在“说明”字段内为此电源控制接口键入可选说明。

e. 单击“确定”将接口添加到节点。将返回到“添加节点”或“节点配置文件”屏幕。

对于 IPMI 电源控制连接

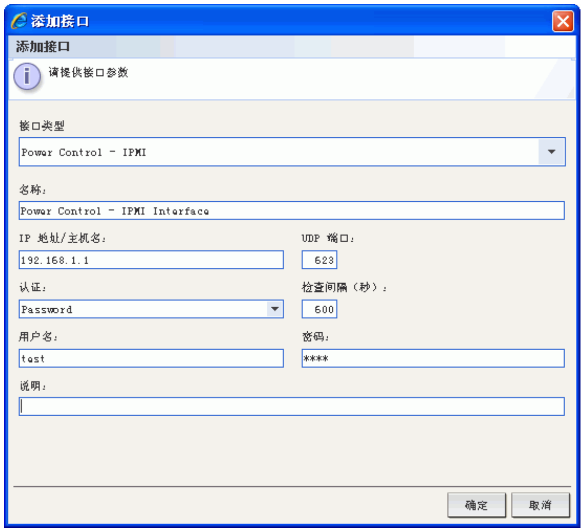


图 69 配置 IPMI 电源控制接口

a. 在“IP 地址/主机名”字段中键入此接口的 IP 地址或主机名。

b. 在“UDP 端口”字段中为此接口键入 UDP 端口。

c. 单击“认证”下拉菜单，选择一种认证方案用于连接此接口。

d. 在“检查间隔（秒）”字段中为此接口键入检查间隔。

e. 在“用户名”字段内为此接口键入用户名。

f. 根据需要在“密码”字段内为此接口键入密码。

g. 单击“确定”将接口添加到节点。将返回到“添加节点”或“节点配置文件”屏幕。

添加接口结果

添加接口后，接口将会出现在“添加节点”或“节点配置文件”屏幕的“接口”表和“默认接口”下拉菜单中。在建立到节点的连接时，可单击该下拉菜单选择要使用的默认接口。

对“添加节点”或“节点配置文件”屏幕的更改保存后，接口的名称也将出现在节点列表中，嵌套于它提供访问的目标节点之下。

连接节点

节点有了接口以后，即可通过该接口用多种方式连接该节点。详情参阅 Raritan 的《CommandCenter Secure Gateway 用户指南》。

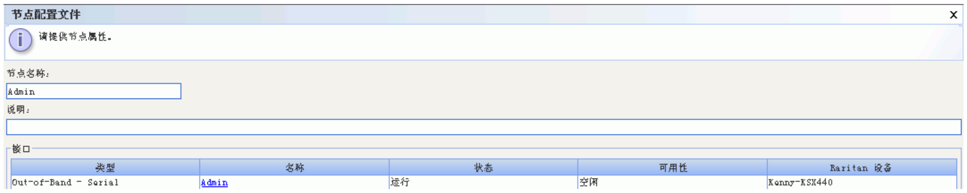


图 70 连接节点的已配置接口

1. 单击“节点”选项卡。
2. 选择要连接的节点。出现“节点配置文件”屏幕。
3. 在“接口”表内，单击要连接的接口的名称。

或者：

1. 在“节点”选项卡内，单击要连接节点旁边的 + 符号展开下面的接口列表。
2. 双击要连接的接口的名称。

编辑接口

要编辑接口：

1. 单击“节点”选项卡。
2. 单击含有要编辑接口的节点。出现“节点配置文件”屏幕。
3. 在“接口”表内，选择要编辑的接口的行。
4. 单击“编辑”。出现“编辑接口”屏幕。

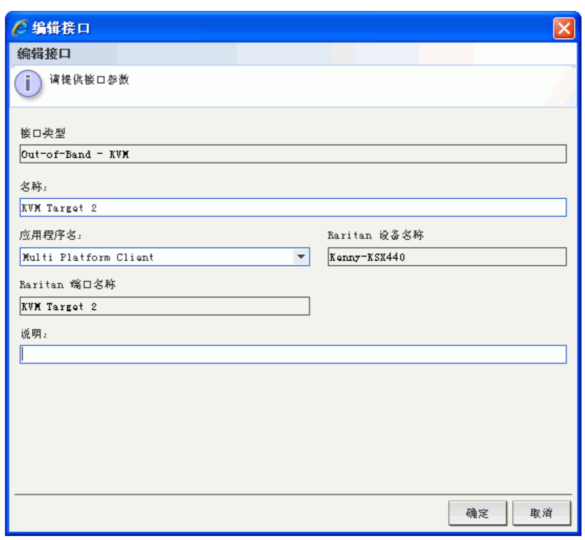


图 71 编辑接口

5. 不能更改现有接口的类型。可更改“接口名称”、“说明”以及该类型其它字段中的值。详情参阅上节“添加接口”。

删除接口

要从节点中删除接口：

1. 单击“节点”选项卡。
2. 单击含有要删除接口的节点。出现“节点配置文件”屏幕。
3. 在“接口”表内，单击要删除的接口的行。
4. 单击“删除”。将会提示进行确认。
5. 单击“是”删除接口。

Ping 节点

可从 CC-SG Ping 节点以确认连接有效。

1. 单击“节点”选项卡，然后选择要 Ping 的节点。
2. 在“节点”菜单中，选择“Ping 节点”。屏幕内出现 Ping 结果。

编辑节点

可以编辑在“节点”选项卡内出现的当前节点。要编辑节点：

1. 单击“节点”选项卡，然后选择要编辑的节点。出现“节点配置文件”屏幕。

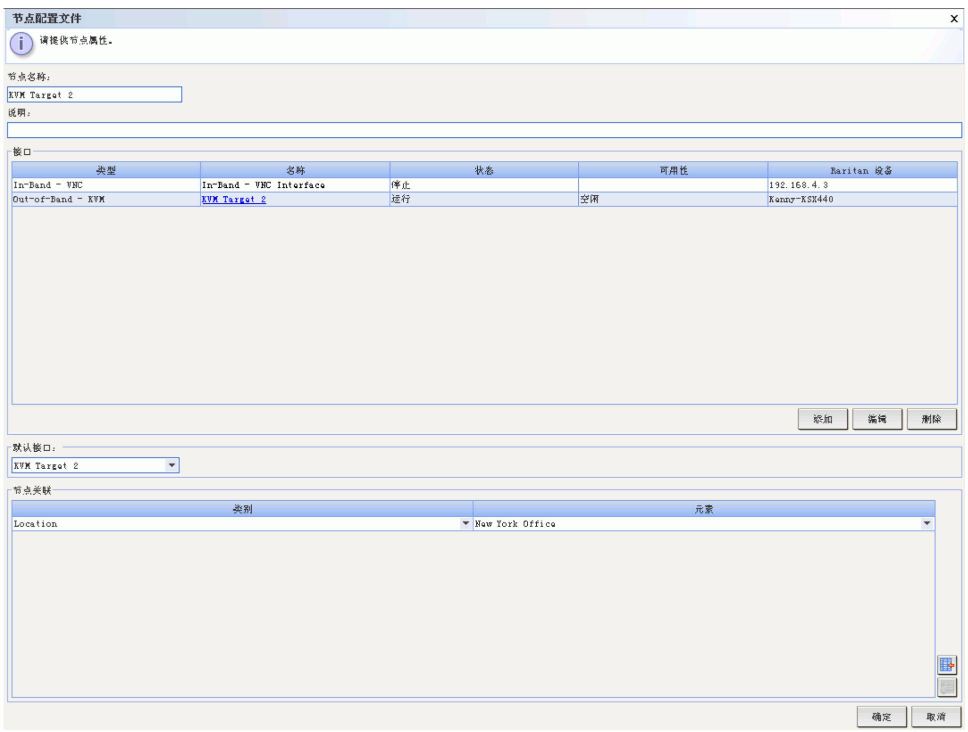


图 72 编辑节点屏幕

2. 如果需要，在“节点名称”字段内键入节点的新名称。在 CC-SG 内所有节点名称必须是唯一的。
3. 在“说明”字段内为此节点键入新的可选简短说明。
4. 在“接口”区域内，单击“添加”添加新接口。有关此过程的详细信息，请参阅上节“添加接口”。
5. 从“接口”表中选择现有节点，然后单击“编辑”或“删除”即可编辑该接口或从节点中删除。有关此过程的详细信息，请参阅上节“编辑接口”或“删除接口”。

6. 可配置一个类别和元素列表，更好地描述和组织此节点。类别是一种节点分类方法，而元素是该分类的具体值。例如，如果节点代表工程部门（名为“部门”的类别）的一台 PC，则可选择名为“工程”的元素。要为节点配置类别和元素：
    a. 对于列表中要指定值的类别，双击旁边的“元素”字段。字段变成一个下拉菜单。
    b. 单击该下拉菜单，选择所需的元素值。如果不想使用此类别，则选择“无”。

    如果看不到要使用的类别或元素值，可通过“关联”菜单进行添加。有关创建类别和元素的详细信息，请参阅**第 4 章：创建关联**。
7. 配置节点完成以后，单击“确定”。

删除节点

删除节点将从节点列表中删除该节点。用户将无法再访问此节点，节点也将丢失所有以前的接口和关联。

要删除节点：

1. 单击左边的“节点”选项卡。
2. 右键单击要删除的节点，选择“删除节点”。出现“删除节点”屏幕，显示所选节点的名称。

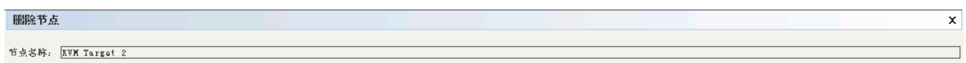


图 73 删除节点

3. 单击“确定”删除节点，或单击“取消”不删除退出。

聊天

对于同一个节点上连接的用户，聊天提供了一种相互交流的方式。要开始节点的聊天会话，必须要连接到该节点。只有同一个节点上的用户能够彼此聊天。

要预定聊天会话：

1. 单击左边的“节点”选项卡。
2. 右键单击当前连接的节点，选择“聊天”，然后单击“开始聊天会话”（如果尚未创建会话）。将会创建一个“聊天”会话。

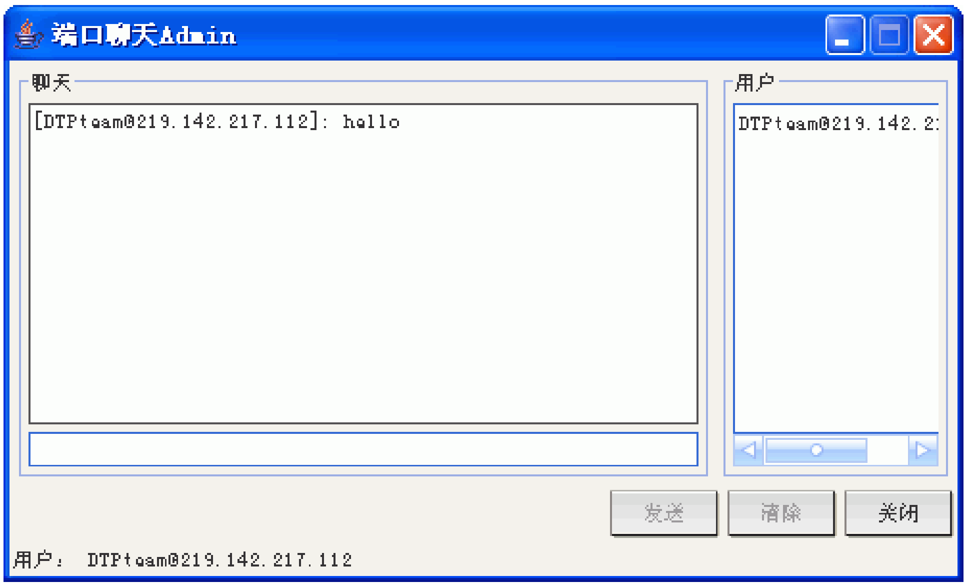


图 74 节点的聊天会话

如果某个聊天正在进行，右键单击该节点，选择“聊天”，然后选择“显示聊天会话”即可加入该聊天会话。

将出现聊天会话窗口，左侧为消息字段，右侧为聊天会话中的用户列表。

3. 在新消息（左下方）字段中键入一条消息，然后按回车键或单击“发送”。消息将出现在聊天（左上方）字段中，供所有用户阅读。
4. 单击“清除”可清除新消息字段中键入但尚未发送的任何消息。此操作不会清除聊天字段。
5. 单击“关闭”离开或结束聊天会话。
6. 如果要关闭聊天会话，则会出现提示。单击“是”关闭所有参与者的聊天会话，单击“否”退出聊天会话但仍为其他人运行。

从节点选项卡中也可关闭所有参与者的聊天会话。右键单击进行聊天会话的节点，选择“聊天”，然后选择“结束聊天会话”。

节点组

节点组允许管理员创建节点的逻辑组，可任意创建或者基于类别和元素创建，以供创建访问策略时使用。有关创建节点组以及将组应用到策略的详细信息，请参阅**第 8 章：策略**。

通过右键单击和选择“节点组”，即可从“节点”列表中访问“节点组”窗口。

此页专门留白。

第 7 章：添加和管理用户和用户组

“用户”构成连接 CC-SG 从而访问节点和管理设备的各个用户和管理员。“用户组”是为其成员用户定义权限集的组织，用户本身是没有权限的。通常，所有用户都必须隶属于用户组。

CC-SG 维护自己的集中用户列表和用户组，用于认证和授权，这将在本章予以介绍。使用外部认证方案（例如 RADIUS 或 Active Directory）时，用户组和策略（参见**第 8 章：策略**）仍需要在 CC-SG 上创建。配置 CC-SG 使用外部认证的相关内容将在**第 9 章：远程认证**中介绍。

用户树

单击“用户”选项卡显示用户树。

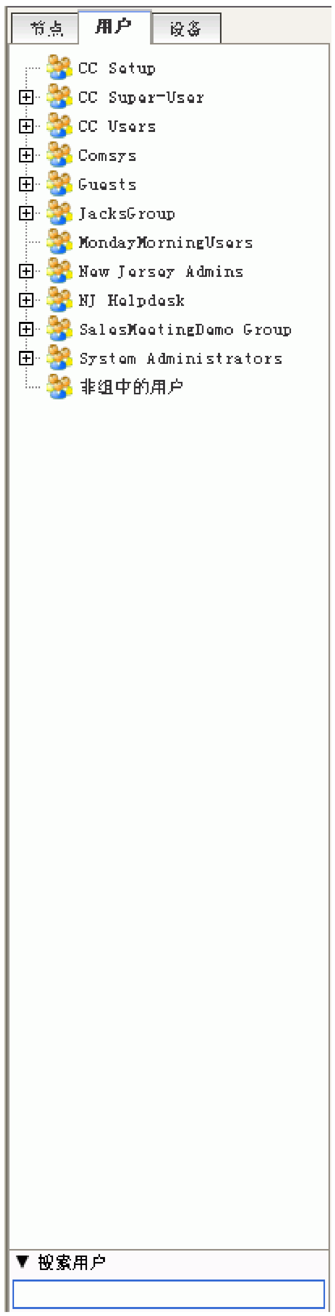


图 75 用户树

用户树显示 CC-SG 内的所有用户组和用户。用户内嵌于所属的用户组之下。含有所分配用户的用户组在列表中显示时旁边有一个 + 符号。单击该符号可展开或隐藏成员用户列表。当前登录到 CC-SG 中的活动用户显示为粗体。

用户树允许在树内搜索用户。搜索方法可在“我的配置文件”屏幕中配置，这将在本章予以介绍。

特殊用户组

CC-SG 默认配置有三个用户组：CC 超级用户、系统管理员和 CC 用户。

CC 超级用户组

“CC 超级用户”组拥有完全的管理和访问权限。此组中只能有一个用户成员。默认用户名为 admin。可以更改默认的用户名。不能删除“CC 超级用户”组。不能更改分配给“CC 超级用户”组的权限、为其添加成员或者删除其中唯一的用户。对“CC 超级用户”组中的成员始终强制使用严格密码。

系统管理员组

“系统管理员”组拥有完全的管理和访问权限。与“CC 超级用户”组不同，可以更改其权限、添加或删除成员。

CC 用户组

“CC 用户组”有带内和带外节点访问权。可更改其权限、添加或删除成员。

非组中的用户

“非组中的用户”没有权限，不能在其中创建用户，也不能将用户手动移到此组中。用户从所有其它现有的用户组中删除时，将被分配到此组中。

重要事项！本章中的很多命令只有先选择了合适的用户组时方能选择。

本节介绍的很多菜单栏命令可通过快捷菜单进行访问，即右键单击用户组或用户，然后从显示的快捷菜单中选择命令。

添加用户组

先创建用户组有助于在添加用户时对其进行组织。创建用户组时，将会为用户组分配一个权限集。分配到该组中的用户将会继承这些权限。例如，如果创建一个组并分配“用户管理”权限，则所有分配到该组的用户将能够看到和执行“用户管理器”菜单中的命令。有关每个权限含义的更多信息，请参阅**附录 D：SNMP 陷阱**。

配置用户组包括四个基本步骤：

- 为组命名并提供说明。
- 选择用户组将要拥有的权限。
- 选择用户组可用来访问节点的接口类型。
- 选择描述用户组可访问哪些节点的策略。

要创建新用户组：

1. 从“用户”菜单中，选择“用户组管理器”，然后单击“添加用户组”。出现“添加用户组”屏幕。

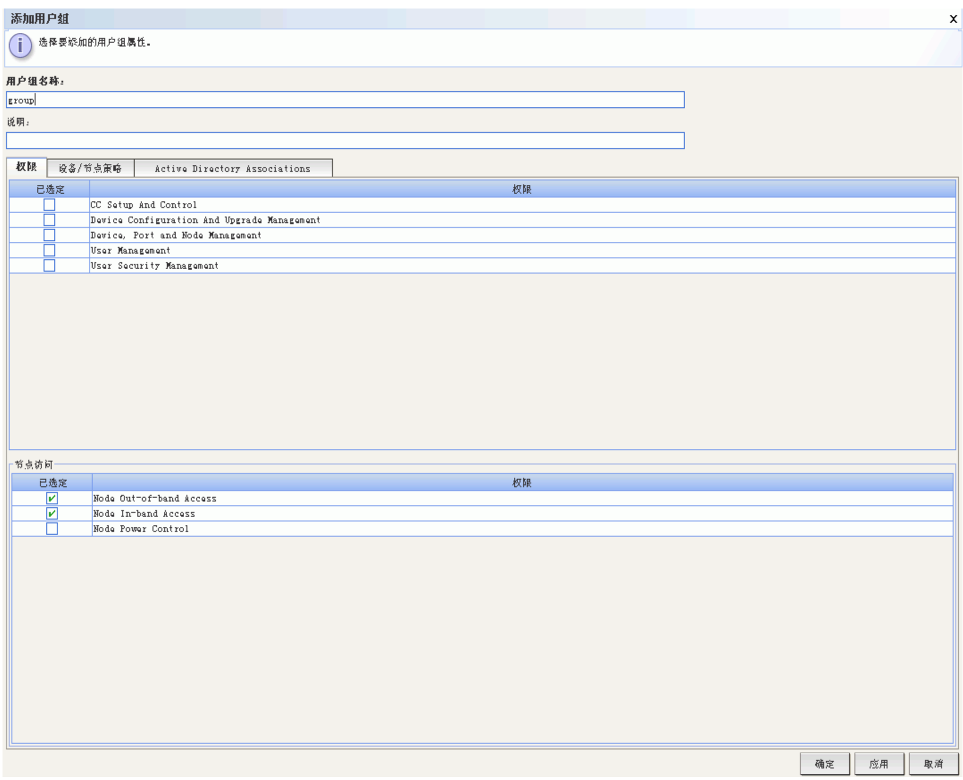


图 76 添加用户组屏幕

2. 在“用户组名称”字段内键入用户组的名称。用户组名称必须是唯一的。
3. 在“说明”字段内为此组键入可选的简短说明。
4. 单击“权限”选项卡。
5. 对于要分配到用户组的每个权限，选中其对应的复选框。
6. 在权限选项卡的下面是“节点访问”区域，含有三种节点访问权限：“节点带外访问”、“节点带内访问”和“节点电源控制”。对于要分配到用户组的每种节点访问类型，选中其对应的复选框。

7. 单击“设备/节点策略”选项卡。出现一个策略表。

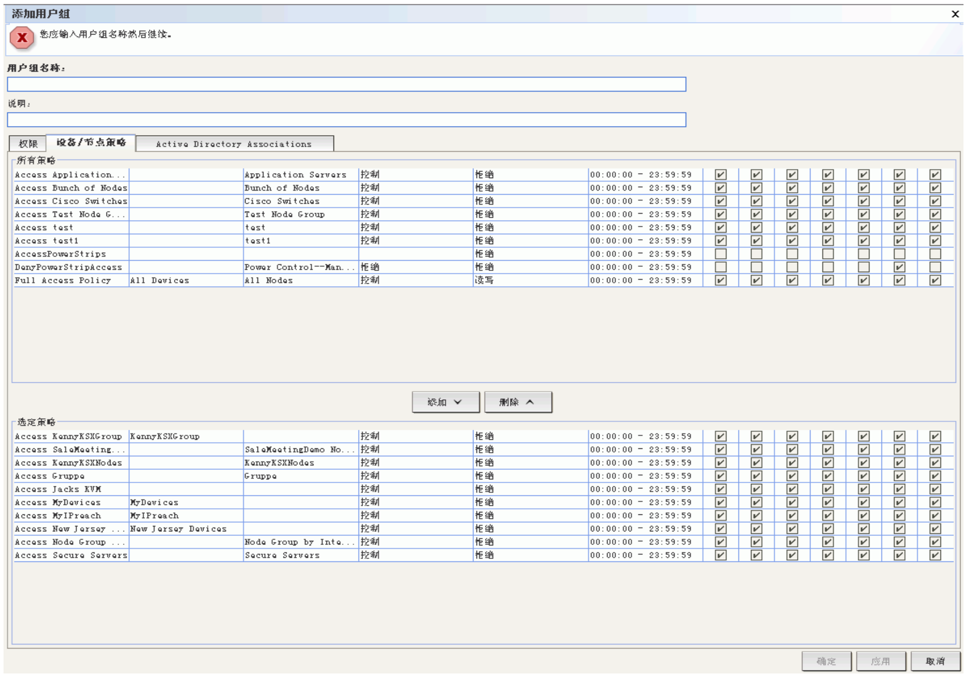


图 77 添加用户组屏幕上的策略选项卡

“所有策略”表列出 CC-SG 上可用的所有策略。每个策略代表一条允许（或拒绝）访问某组节点的规则。有关策略以及如何创建的详细信息，请参阅**第 8 章：策略**。

8. 在“所有策略”列表中，选择要指定给用户组的策略，然后单击“添加”将策略移到“已选定策略”列表中。“已选定策略”列表中的策略将允许或拒绝用户对此策略所控制的节点（或设备）的访问。
9. 重复此步骤将其它策略添加到用户组。
10. 如果要简单地允许此组访问所有的可用节点，请选择“添加策略”列表中的“完全访问策略”，然后单击“添加”。
11. 如果需要从用户组中删除某个策略，请从“已选定策略”列表选择该策略名称，然后单击“删除”。
12. 为此组配置策略完成后，单击“应用”保存此组并创建其它用户组，或者单击“确定”保存此组并结束创建。如果单击“应用”，重复本节中的步骤添加其它用户组。

编辑用户组

编辑用户组可更改该组的现有权限和策略。

注：对于“CC 超级用户”组和“非组中的用户”组，不能编辑权限或策略。

要编辑组：

1. 单击左边的“用户”选项卡。
2. 单击“用户”选项卡中的用户组。出现“用户组配置文件”。

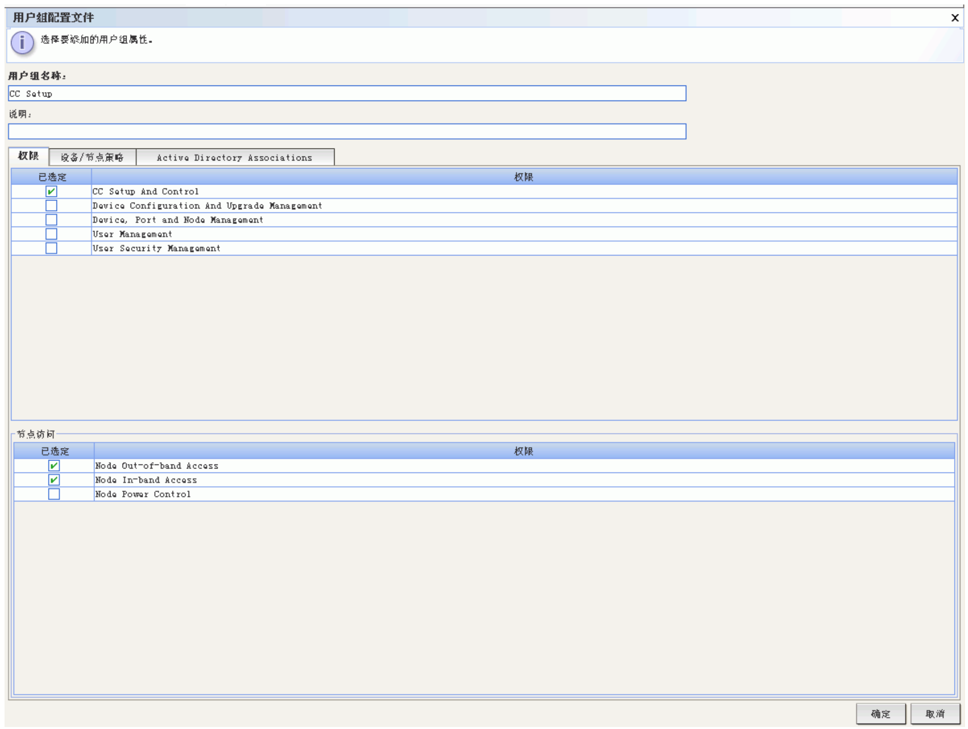


图 78 编辑选定的组

3. 如果需要，在“用户组名称”字段内键入用户组的新名称。
4. 在“说明”字段内为用户组键入新的可选简短说明。
5. 单击“权限”选项卡。
6. 对于要分配到用户组的每个权限，选中其对应的复选框。取消选择某个权限即将其从组中删除。
7. 在“节点访问”区域内，单击下拉菜单查看想要此组访问时通过的接口类型，然后选择“控制”。
8. 单击下拉菜单查看不要此组访问时通过的接口类型，然后选择“拒绝”。
9. 单击“策略”选项卡。将出现两个策略表。
10. 对于每个要添加到组中的策略，从“所有策略”中选择策略，然后单击“添加”将策略移到“已选定策略”列表中。“已选定策略”列表中的策略将允许或拒绝用户对此策略所控制的节点（或设备）的访问。
11. 如果需要从用户组中删除某个策略，请从“已选定策略”列表选择该策略名称，然后单击“删除”。
12. 为此组配置策略完成后，单击“确定”保存对组的更改，或单击“取消”退出而不保存。

删除用户组

删除用户组即将该组从 CC-SG 中删除。被删除组内的用户将保留在曾被指定的其它组内。如果被删除组内的用户不在其它任何组内，将被分配到“非组中的用户”组内，没有分配任何权限。

要删除用户组：

1. 单击左边的“用户”选项卡。
2. 单击“用户”选项卡中要删除的用户组。
3. 从“用户”菜单中，选择“用户组管理器”，然后单击“删除用户组”。出现“删除用户组”屏幕。

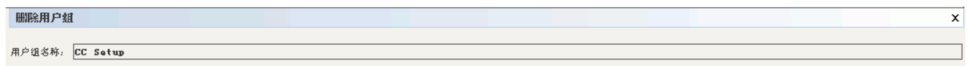


图 79 删除用户组

4. 单击“确定”删除用户组，或单击“取消”退出而不删除组。

单击“确定”后，将出现一条状态消息，确认组已成功删除。

添加用户

将用户添加到组即分配用户在 CC-SG 中的访问权限。用户访问节点或管理设备的能力将取决于他们被添加到什么样的用户组。

要添加用户：

1. 单击左边的“用户”选项卡。
2. 在“用户”选项卡内单击要添加用户的用户组（不选择组就不能添加用户）。
3. 从“用户”菜单中，选择“用户管理器”，然后单击“添加用户”。出现“添加用户”屏幕。

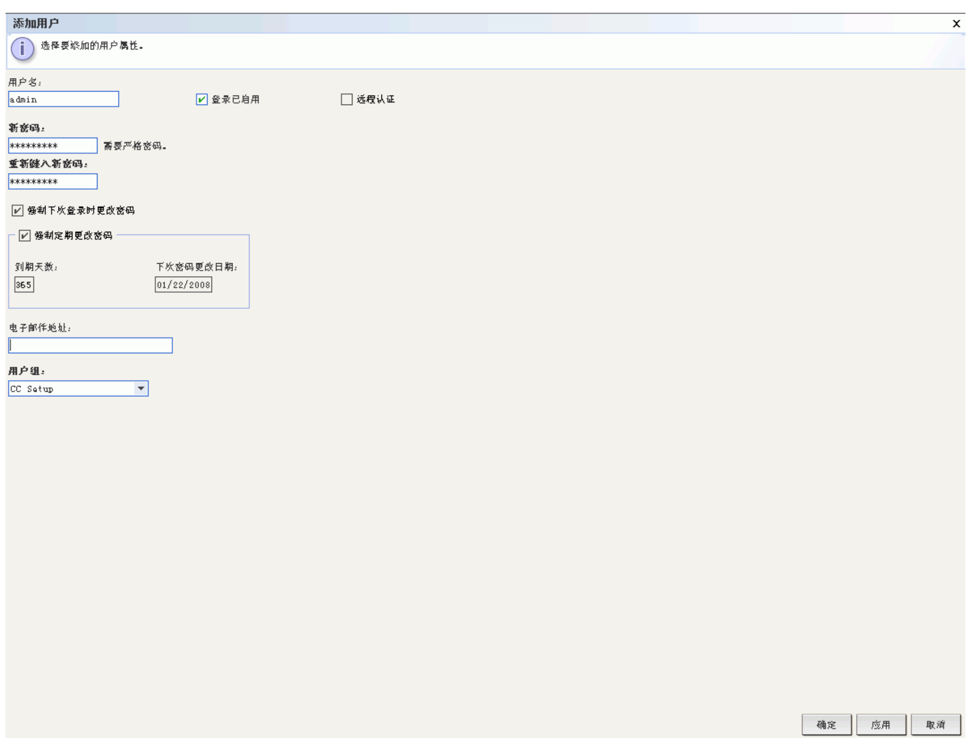


图 80 添加用户

4. 在“用户名”字段中，键入要添加的用户的名称，此名称将用于登录 CC-SG。
5. 如果想要此用户能够登录 CC-SG，则选中“登录已启用”。
6. 只有在用户需要通过外部服务器进行认证（例如 TACACS+、RADIUS、LDAP 或 AD），选中“远程认证”。如果使用远程认证，则不需要密码，“新密码”和“再次键入新密码”字段将被禁用。
7. 在“新密码”和“重新键入新密码”字段中，键入用户登录 CC-SG 时所用的密码。

---

*注：如果启用严格密码，则输入的密码必须要符合已经建立的规则。屏幕顶部的信息栏将显示消息帮助了解密码要求。有关严格密码的详细信息，参见**第 12 章：高级管理**。*

---

8. 如果想要强制用户在下次登录时更改所分配的密码，则选中“强制下次登录时更改密码”。
9. 如果想要指定强制用户多久更改一次密码，则选中“强制定期更改密码”。
   a. 如果选中，在“到期周期（天）”字段中，键入强制用户更改密码之前可使用的天数。
10. 在“电子邮件地址”字段内，键入用户的电子邮件地址。此地址将用于发送用户通知。
11. 如果要更改添加此用户的组，单击“用户组”下拉菜单并选择一个新组。
12. 配置此用户完成后，单击“应用”保存此用户并创建其他用户，或者单击“确定”保存此用户并结束创建。所创建的用户将出现在“用户”选项卡内，内嵌于所隶属的用户组下面。

编辑用户

要编辑用户：

1. 单击左边的“用户”选项卡。
2. 单击要编辑用户所在用户组旁边的 + 符号。
3. 单击要编辑的用户。出现“用户配置文件”。

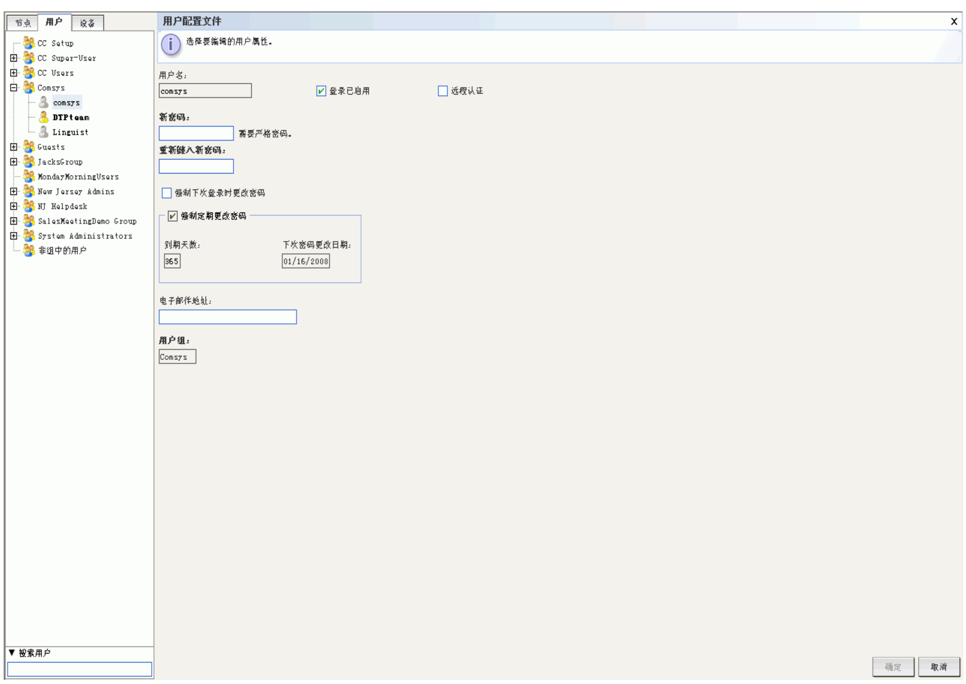


图 81 编辑选定的用户

4. 如果要禁止此用户登录 CC-SG，则取消选取“登录已启用”。如果要允许此用户登录 CC-SG，则选中“登录已启用”。
5. 只有在用户需要通过外部服务器进行认证（例如 TACACS+、RADIUS、LDAP 或 AD），选中“远程认证”。如果使用远程认证，则不需要密码，“新密码”和“再次键入新密码”字段将被禁用。
6. 在“新密码”和“再次键入新密码”字段中，键入新密码更改此用户的密码。

注：*如果启用严格密码，则输入的密码必须要符合已经建立的规则。屏幕顶部的信息栏将帮助了解密码要求。有关严格密码的详细信息，参见****第 12 章：高级管理****。*

7. 如果想要强制用户在下次登录时更改所分配的密码，则选中“强制下次登录时更改密码”复选框。
8. 在“电子邮件地址”字段中，键入一个新的电子邮件地址添加该地址，或者更改用户已配置的电子邮件地址。此地址将用于发送用户通知。
9. 此用户编辑完成后，单击“确定”保存对用户的更改，或单击“取消”退出而不保存。

注：*编辑用户时不能更改所隶属的组。详情参阅下面的“将用户添加到组”。*

删除用户

删除用户组即将该用户从 CC-SG 中完全删除。这可用于删除不再需要的帐户。

要删除用户：

1. 单击左边的“用户”选项卡。
2. 单击要删除用户所在用户组旁边的 + 符号。
3. 单击要删除的用户。
4. 从“用户”菜单中，选择“用户管理器”，然后单击“删除用户”。出现“删除用户”屏幕。

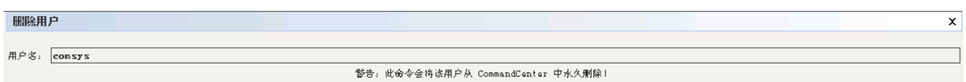


图 82 删除用户

5. 单击“确定”从 CC-SG 中永久性删除用户，或单击“取消”不删除退出。

注：*此命令将删除用户的所有实例，即使用户存在于多个用户组内。如果仅想从一个组内删除用户，请参阅下面的“从组中删除用户”。*

将用户分配到组

此命令用于将现有用户分配到当前尚不隶属的组。用这种方式分配的用户将被添加新组内，同时仍然存在于以前所分配的任何组内。要移动用户，可联合使用此命令以及下面介绍的“从组中删除用户”。

要将用户分配到组：

1. 单击左边的“用户”选项卡。
2. 单击要分配用户的用户组。
3. 从“用户”菜单中，选择“用户组管理器”，然后单击“将用户分配到组”。出现“将用户分配到组”屏幕。

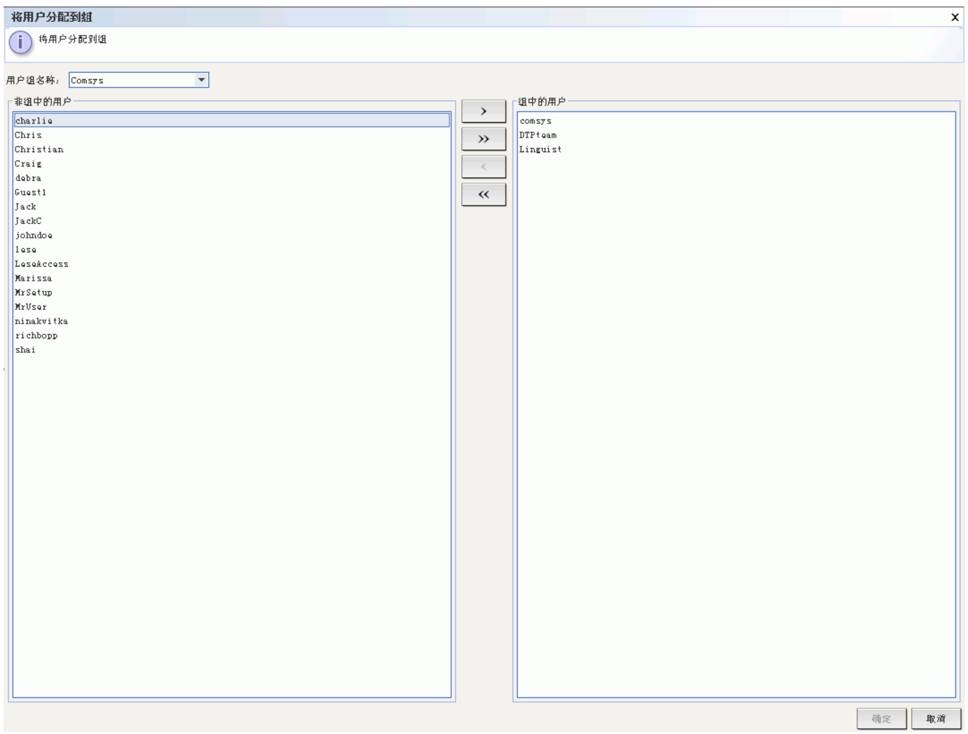


图 83 将用户添加到组屏幕

4. 尚未被分配到目标组的用户出现在“非组中的用户”列表内。从此栏内选择要添加的用户，然后单击 > 按钮将其移到“组内用户”列表。
5. 单击 >> 按钮将所有未在组内的用户移到“组内用户”列表。
6. 要从目标组内删除用户，请在“组内用户”列表中选择要删除的用户，然后单击 < 按钮。
7. 单击 << 按钮从“组内用户”列表中删除所有用户。
8. 当所有用户都被移到到合适的栏内时，单击“确定”。“组内用户”列表中的用户将被添加到所选的用户组。

从组中删除用户

此命令从所选的组内删除一个选定用户。此命令不会从其它任何组内删除该用户，也不会从 CC-SG 中删除该用户。

要从组中删除用户：

1. 单击左边的“用户”选项卡。
2. 单击要删除用户所在用户组旁边的 + 符号。

3. 单击要删除的用户。
4. 从“用户”菜单中，单击“用户管理器”，然后单击“从组中删除用户”。出现“删除用户”，显示该用户以及要从中删除的组。

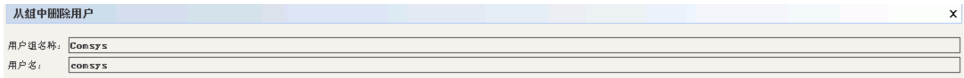


图 84 从组中删除用户

5. 单击“确定”从组中删除用户，或单击“取消”退出而不删除用户。

注：如果从组中删除用户，并且用户不隶属任何其它组，则会被添加到“非组中的用户”组。

其它用户和用户组功能

我的配置文件

“我的配置文件”允许所有用户查看其当前帐户的详细信息、更改部分详细信息和自定义可使用性设置。这是 admin 帐户更改帐户名的唯一方法。

要编辑用户配置文件：

1. 在“Secure Gateway”菜单上，单击“我的配置文件”。出现“更改我的配置文件”屏幕，显示帐户的详细信息。

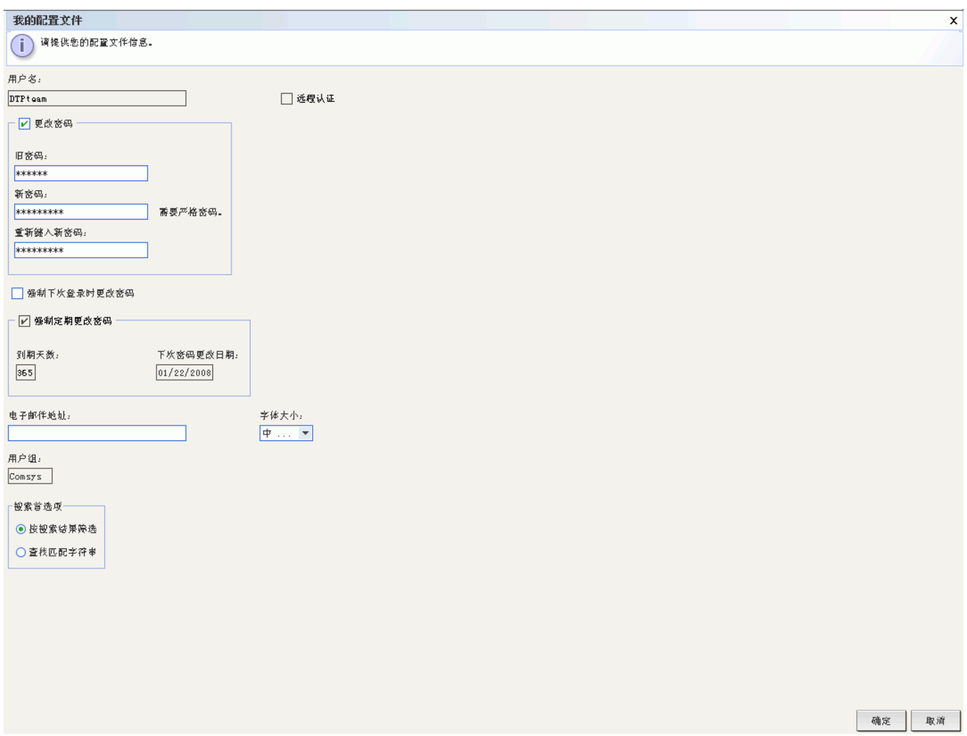


图 85 我的配置文件屏幕

2. 如果在 admin 帐户上登录，则可以在“用户名”字段中键入新的名称来更改帐户名称。
3. 如果要更改密码，则选中“更改密码”。
   a. 在“旧密码”字段内键入当前密码。
   b. 在“新密码”字段内键入新密码。如果要求严格密码，则会出现通知。

c. 在“重新键入新密码”字段中再次键入新密码。
4. 在“电子邮件地址”字段中键入新地址可添加或更改 CC-SG 用于发送通知的地址。
5. 单击“字体大小”下拉箭头，调整标准 CC-SG 客户端显示所用的字体大小。
6. 在“搜索首选项”区域内，选择搜索节点、用户和设备时使用的首选方法。
   - **按搜索结果筛选**——允许使用通配符，将节点、用户或设备的显示限制于包含搜索标准的所有名称。
   - **查找匹配字符串**——不支持使用通配符，在键入时即突出显示最匹配的节点、用户或节点。单击“搜索”后，列表将限制于那些包含搜索标准的项。
7. 配置文件编辑完成后，单击“确定”保存更改，或单击“取消”退出而不保存。

注销用户

此命令可用于将活动用户从 CC-SG 中注销。可用于注销一个用户组内的所有活动用户。

要注销用户：

1. 单击左边的“用户”选项卡。
2. 单击要注销用户所在用户组旁边的 + 符号。
3. 单击要注销的用户。要注销多个用户，请按住 **Ctrl** 键单击其他用户。
4. 从“用户”菜单中，选择“用户管理器”，然后单击“注销用户”。出现“注销用户”屏幕，内有所选用户的列表。
5. 单击“确定”从 CC-SG 中注销用户，或单击“取消”退出而不注销用户。

要注销一个用户组内的所有用户

1. 单击左边的“用户”选项卡。
2. 单击要注销用户所在的用户组。要注销多个组内的用户，请按住 **Ctrl** 键单击其他组。
3. 从“用户”菜单中，选择“用户组管理器”，然后单击“注销用户”。出现“注销用户”屏幕，内有所选组的活动用户列表。
4. 单击“确定”从 CC-SG 中注销用户，或单击“取消”退出而不注销用户。

批量复制

为了节省时间，可使用“批量复制”将一个用户的权限和策略克隆到多个其他现有用户，方法是将这些用户移到所选用户所在的用户组内。要执行批量复制：

1. 单击左边的“用户”选项卡。
2. 单击要复制用户所在用户组旁边的 + 符号。
3. 单击要复制的用户。
4. 从“用户”菜单中，选择“用户管理器”，然后单击“批量复制”。出现“批量复制”屏幕。

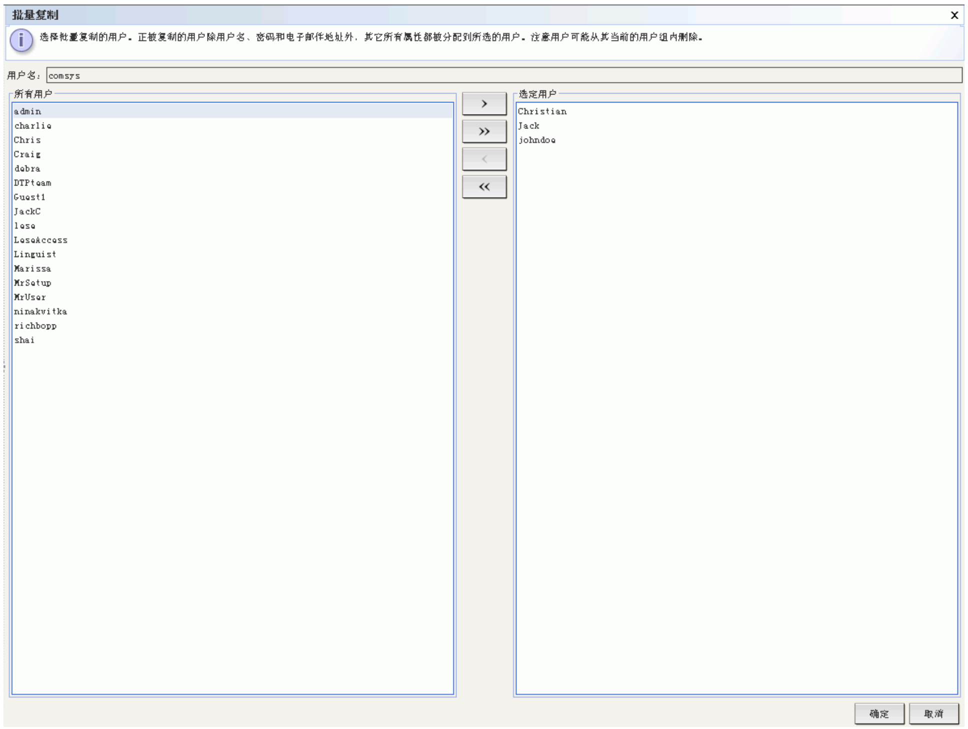


图 86 批量复制屏幕

5. 在“所有用户”列表中，选择将会使用在“用户名”字段中用户配置文件的哪些用户。
6. 单击 > 按钮将用户名移到“选定用户”列表。
7. 单击 >> 按钮将所有用户移到“选定用户”列表。
8. 要从“选定用户”列表中删除用户，请选择该用户并单击 < 按钮。
9. 单击 << 按钮从“组内用户”列表中删除所有用户。
10. 单击“确定”复制用户属性。被复制的用户将从现有组被移到所选用户隶属的组。

第 8 章：策略

使用策略控制访问

配置新策略来提供用户到节点的访问是可选操作，但却是有效使用 CC-SG 来控制这种访问的核心。如果要将所有用户访问给予所有节点，只需简单地将“完全访问策略”分配给所有用户组即可。

如果要对用户的节点访问有更多控制，则需要创建策略来定义访问的规则。与所有权限类似，策略被分配到用户组，从而将其中的访问规则应用到组内的用户。

如果完成“指导设置”（参见**第 3 章：使用指导设置配置 CC-SG**），则可能已经创建多个基本策略。现在要将这些策略应用到现有的用户组。如果未曾使用“指导设置”或者尚未创建所需的策略，则应遵照以下指导说明。操作如下：

- 创建节点组来组织要为其创建访问规则的节点。
- 创建设备组（如果要为向节点提供接口的 Raritan 设备创建访问规则）。
- 为节点（或设备）创建策略，指定何时能够访问该节点。
- 将此策略应用到用户组。

策略摘要

下图直观地介绍如何实现 CC-SG 的安全性：

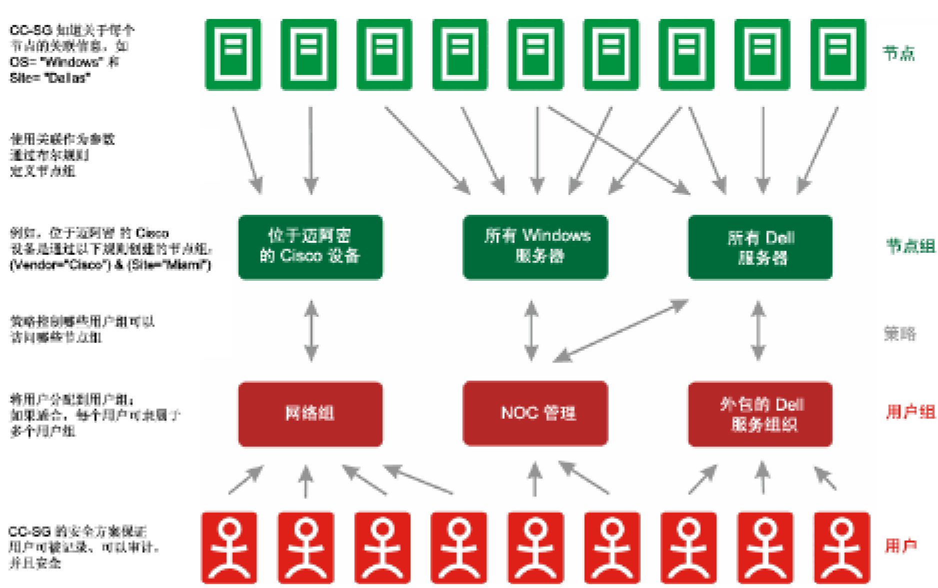


图 87 策略摘要

节点组

节点组用于将节点组织成一个集合。然后，此组将成为策略的基础，不论是允许还是拒绝对此特殊节点集合的访问。节点可任意分组，或者按一套共同属性进行分组。

或者，如果曾使用关联管理器为节点创建类别和元素，则已经创建了按照公共属性组织节点的方法。CC-SG 基于这些元素自动创建默认的访问策略。有关创建类别和元素的详细信息，请参阅**第 4 章：关联**。

要查看现有节点组：

在“关联”菜单中，单击“节点组”。显示“节点组管理器”窗口。左侧显示现有节点组列表，主面板中显示所选节点组的详细信息。

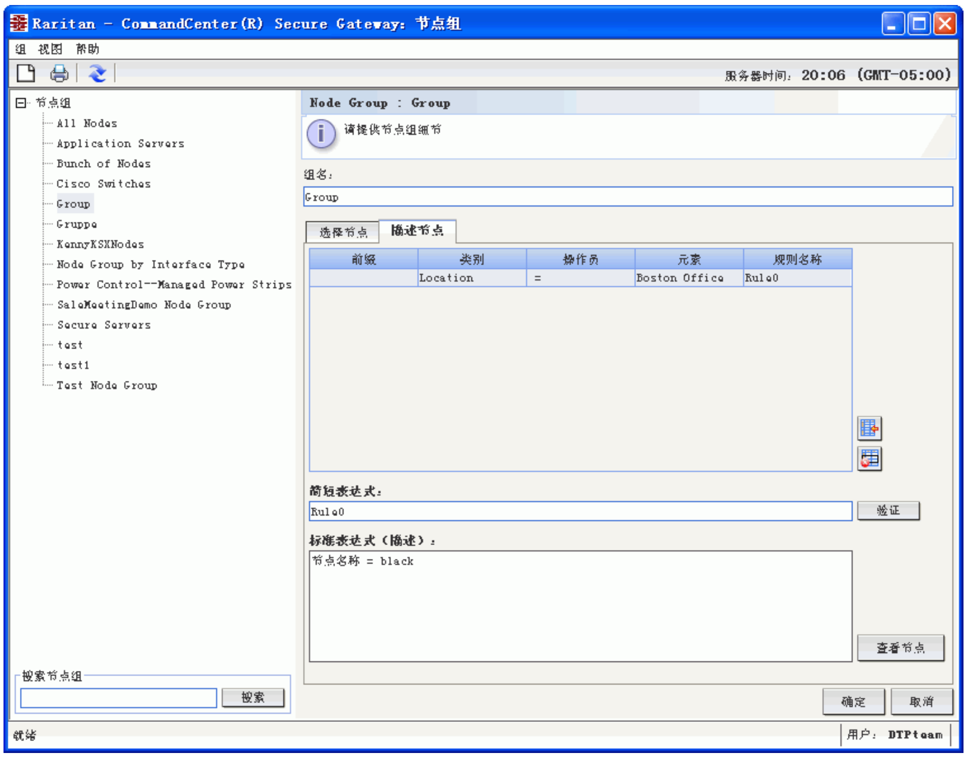


图 88 节点组管理器

1. 左侧显示现有节点组列表。单击一个节点组可在节点组管理器中查看组的详细信息。

   如果组为任意形成，则会显示“选择节点”选项卡，显示足内节点列表和不在组中的节点。

   如果组是基于共同属性形成的，则显示“描述节点”选项卡，显示管理为组选择节点的规则。

2. 要在节点组列表内搜索节点，在列表底部的“搜索”字段中键入一个字符串，然后单击“搜索”。搜索方法通过“我的配置文件”屏幕进行配置。详情参见**第 7 章：用户和用户组**。

3. 如果基于属性查看组，单击“查看节点”显示节点组内当前的节点列表。将出现“节点组内节点”窗口，显示节点及其全部属性。

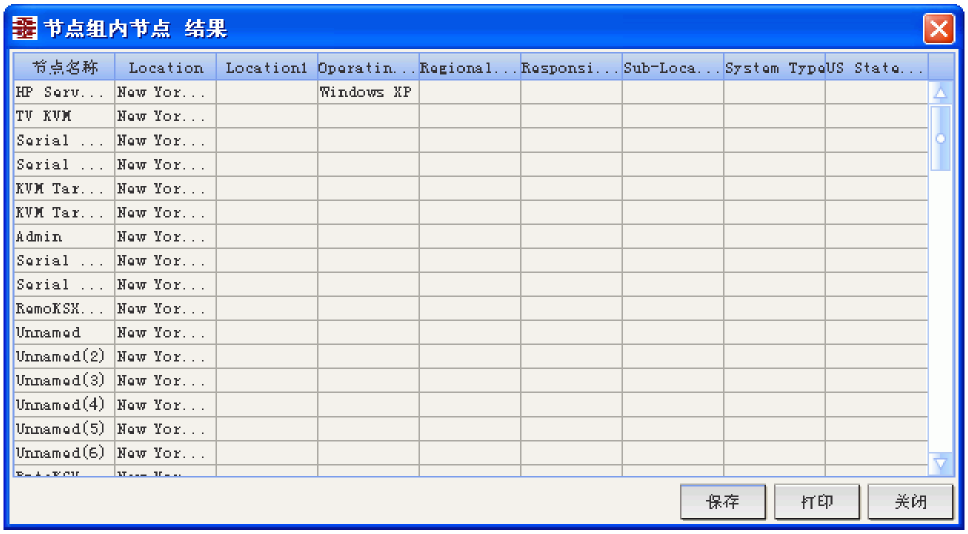


图 89 基于属性的组内节点

添加节点组

要添加新的节点组：

1. 在“关联”菜单中，单击“节点组”。显示“节点组管理器”窗口。
2. 在“组”菜单上，单击“添加”。将出现节点组模板。
3. 在“组名称”字段中，为要创建的节点组键入名称。

将节点添加到组可通过两种方式：“选择节点”和“描述节点”。“选择节点”方法允许通过从可用节点列表中选择节点，将节点任意分配给组。“描述节点”方法允许指定描述节点的规则，参数符合这些描述的节点将被添加到组中。

选择节点

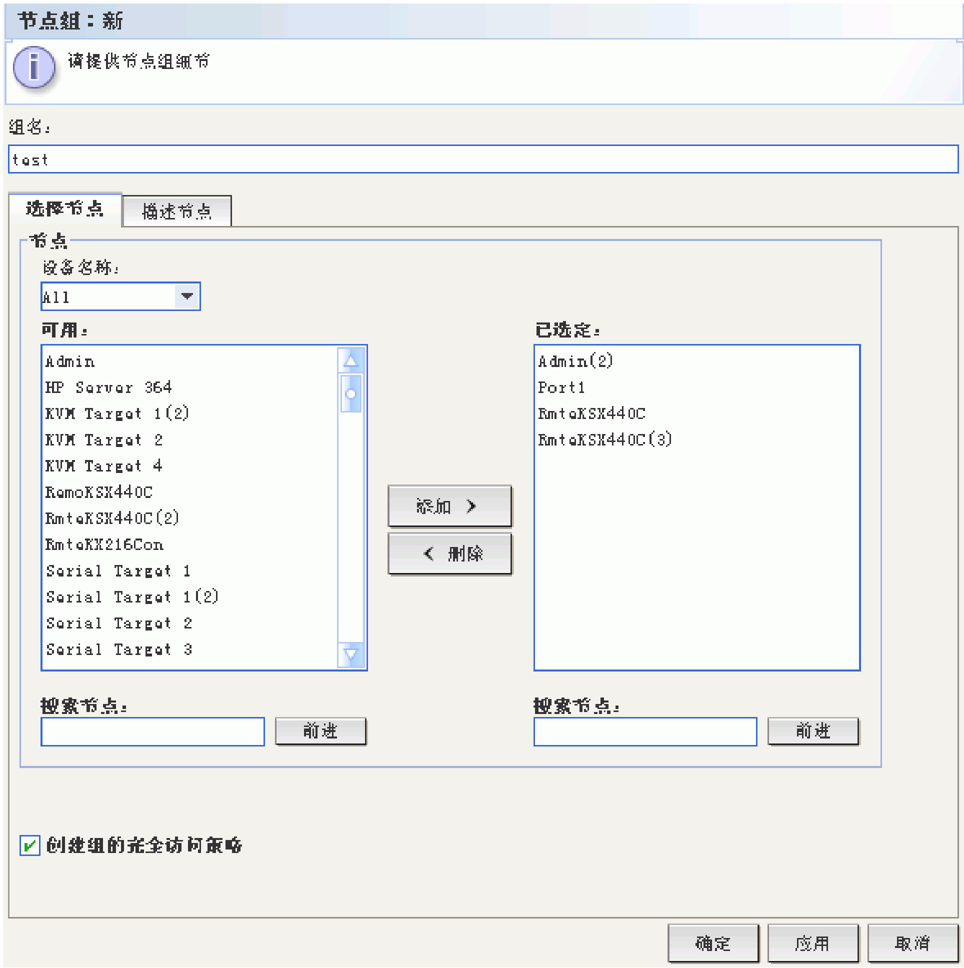


图 90 使用所选节点添加节点

1. 单击“选择节点”选项卡。
2. 如果要过滤“可用”列表仅显示带该设备接口的节点，单击“设备名称”下拉菜单并选择一个设备。
3. 在“可用”列表中选择要添加到组中的节点，然后单击“添加”将节点移到“已选定”列表中。“已选定”列表中的节点将被添加到组中。
4. 如果需要从组中删除某个节点，请从“已选定”列表选择该节点名称，然后单击“删除”。
5. 可在“可用”或“已选定”列表中搜索节点。在列表下面的字段中键入搜索术语，然后单击“执行”。
6. 如果要创建一个策略允许在任何时候访问此组内的节点，则选中“创建此组的完全访问策略”。
7. 将节点添加到组完成后，单击“添加”创建节点组。组将被添加到左边的“节点组”列表内。

描述节点

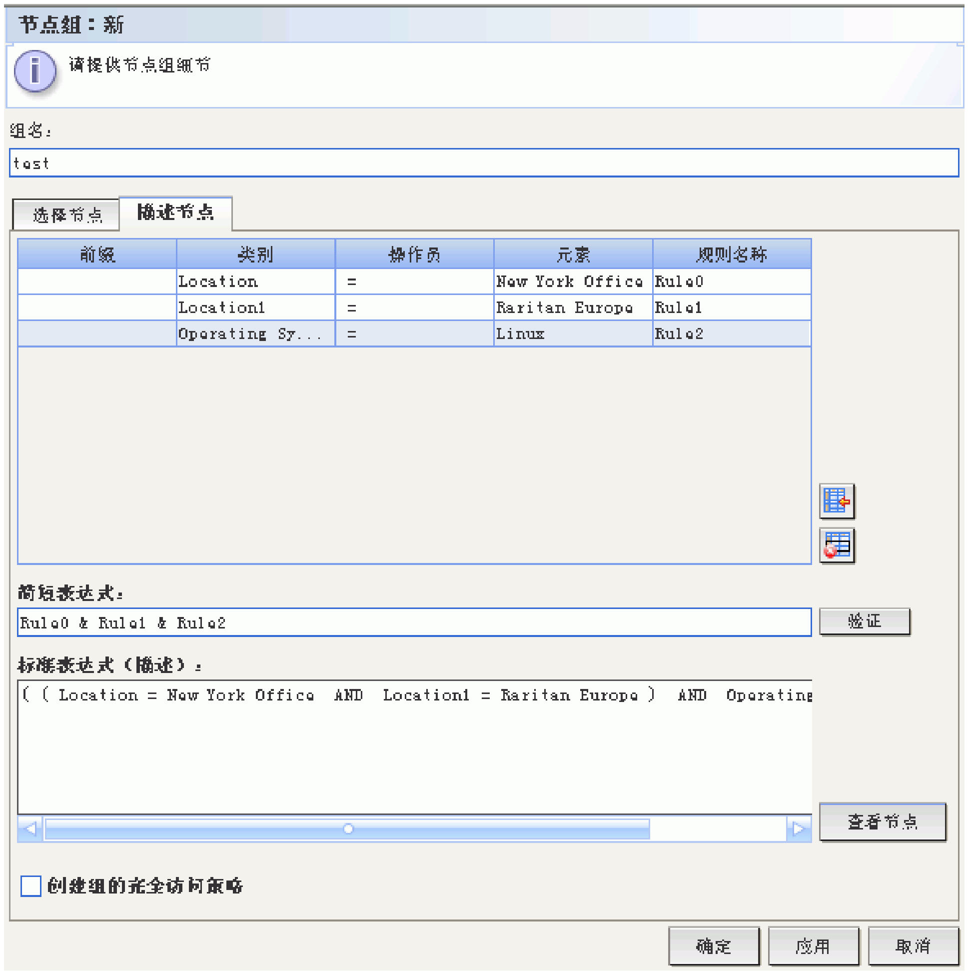


图 91 使用多个规则描述节点组

1. 单击“选择节点”选项卡。
2. 单击“添加新行”在表中添加一行用于新建规则。规则的格式类似表达式，可对节点进行比较运算。
3. 双击行内的每个栏将合适的单元格变成下拉菜单，然后为每个组件选择合适的值：
   - **前缀**——留空或选择“否”。如果选择“否”，此规则将过滤与表达式其他相反的值。
   - **类别**——选择规则中将要评估的一种属性。此处将提供在“关联管理器”中创建的所有类别。同时还包括“节点名称”和“接口”。
   - **运算符**——选择一种在类别和元素项之间要执行的比较运算。提供三种运算符：=（等于）、LIKE（用于在名称中发现元素）以及 <> （不等于）。
   - **元素**——为要比较的类别属性选择一个值。只有与所选类别关联的元素会在此显示（例如：如果评估“部门”类别，则“Location”元素不会在此出现）。
   - **规则名称**——指定给此行内规则的名称。这些值不能编辑。这些值用于在“简短表达式”字段中编写说明。

例如规则 `Department = Engineering` 表示描述类别“部门”设为“工程”的所有节点。这与在“添加节点”操作中配置关联时的情形完全一样。

4. 如果要添加其它规则，再次单击“添加新行”，然后进行必要的配置。配置多个规则可提供多个评估节点的标准，从而进行更为精确的描述。
5. 如果要删除一个规则，请在表中单击该规则，然后单击“删除行”。
6. 规则表仅将标准用于评估节点。要为节点组编写描述，请在“简短表达式”字段中按“规则名称”添加规则。如果描述仅需要一个简单的规则，则只需简单地在字段中键入规则名称即可。如果要评估多个规则，请将规则键入字段中，并使用逻辑运算符集描述规则之间的关系。
    - **& -** “与”运算符。节点必须满足此运算符两侧的规则，描述（或该描述部分）才被评估为真。
    - | - “或”运算符。节点仅需满足此运算符两侧的任一规则，描述（或该描述部分）才被评估为真。
    - (and) – 分组运算符。将描述划分为几个部分，用括号包含。首先评估括号内的部分，然后再将描述的其余部分与节点比较。括号对可内嵌于另一括号对内。

    例如：如果仅想描述隶属于工程部的节点，则创建规则 `Department = Engineering`。这个为 Rule0。然后只需在“简短表达式”字段中键入 Rule0。

    又例如：要描述隶属于工程部或者位于 Philadelphia 的一组节点，并且指定所有设备必须有 1 GB 的内存，则需要开始创建三个规则。`Department = Engineering` (Rule0) `Location = Philadelphia` (Rule1) `Memory = 1GB` (Rule2)。这些规则需要按一定关系排列起来。由于节点可以隶属于工程部或者位于 Philadelphia，因此使用“或”运算符 `|` 连接二者：`Rule0|Rule1`。需要将其放到括号内先进行比较：`(Rule0|Rule1)`。最后，由于节点必须满足此比较结果“并且”要有 1GB 的内存，因此要使用“与”运算符 **&** 将此部分与 Rule2 连接：`(Rule0|Rule1)&Rule2`。然后在“简短表达式”字段中键入这个最终的表达式。

7. 将描述写入“简短表达式”后，单击“验证”。如果描述的格式不正确，则会收到一条警告。如果描述的格式正确，则“标准表达式”字段中将会出现此表达式的标准化格式。
8. 单击“查看节点”查看哪些节点满足此表达式。将出现“节点组内节点”窗口，显示将按当前表达式进行分组的节点。这可用于检查表达式是否正确编写。如果不正确，可返回到规则表或“简短表达式”字段进行修改。
9. 如果要创建一个策略允许在任何时候访问此组内的节点，则选中“创建此组的完全访问策略”。
10. 对隶属此组的节点描述完成后，单击“添加”创建节点组。组将被添加到左边的“节点组”列表内。

编辑节点组

编辑节点组可更改组的成员关系和说明。要编辑节点组：

1. 在“关联”菜单中，单击“节点组”。显示“节点组管理器”窗口。

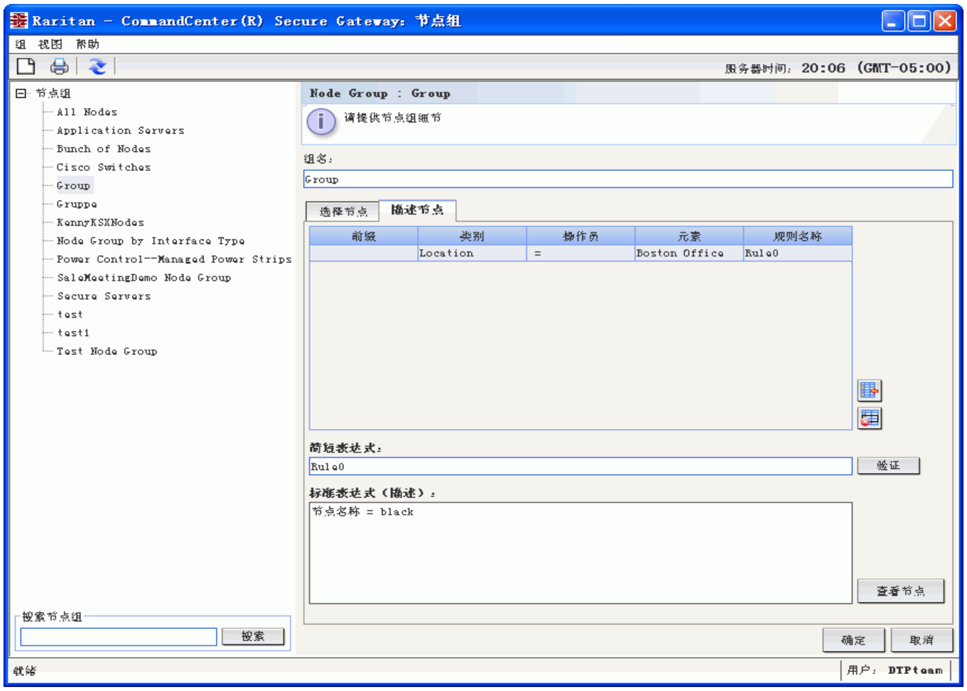


图 92 编辑节点组

2. 在左边的“节点组”列表中单击要编辑的节点。在“节点组”窗口中将出现该节点的详细信息。
3. 有关如何配置节点组的详细信息，请参阅“选择节点”或“描述节点”部分中的说明。
4. 节点组编辑完成以后，单击“编辑”。

删除节点组

1. 在“关联”菜单中，单击“节点组”。显示“节点组管理器”窗口。
2. 在左边的“节点组”列表中单击要删除的节点。
3. 在“组”菜单中，单击“删除”。

设备组

设备组的运行与节点组类似，只是设备组用于将 Raritan 设备组织成集合，用于通过策略进行管理。

详情参见第 5 章：添加设备和设备组中的“设备组管理器”。

策略管理器

创建节点组和设备组以后，即可作为创建访问策略的基础——规则描述用户可以或不可以访问节点组（或设备组）内的节点或设备、此规则何时生效。

添加策略

要创建策略：

1. 从“关联”菜单中，单击“策略”。出现“策略管理器”窗口。

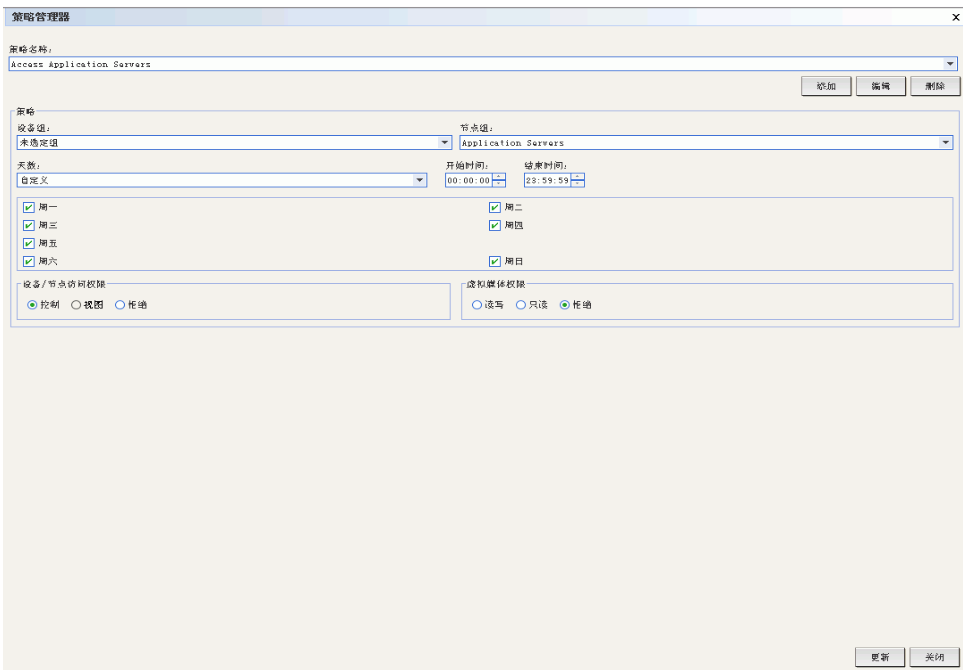


图 93 策略管理器

2. 单击“添加”。出现一个对话窗口，要求输入策略名称。



图 94 添加策略

3. 在“输入策略名称”字段内键入新策略的名称。
4. 单击“确定”。新策略将被添加到“策略管理器”屏幕上的“策略名称”列表内。

5. 单击“设备组”下拉箭头，选择此策略管理对其访问的设备组。
   单击“节点组”下拉箭头，选择此策略管理对其访问的节点组。
   如果策略仅覆盖一种类型的组，则仅为该组选择值。
6. 单击“天”下拉箭头，选择此策略覆盖一周中的哪些天：“全部”天、“工作日”（仅从周一到周五）、“周末”（仅周六和周日）或“自定义”（选择特定天）。
   a. 选择“自定义”可选择自己的天集合。各个天的复选框将被启用。
   b. 对于要此策略覆盖的每一天，选中其对应的复选框。
7. 在“开始时间”字段中，键入此策略开始生效的时间。时间必须是 24 小时格式。
8. 在“结束时间”字段中，键入此策略当天结束的时间。时间必须是 24 小时格式。
9. 在“设备/节点访问权限”字段中，选择“控制”即定义此策略允许在指定的时间和天内对所选节点或设备组进行访问。选择“拒绝”即定义此策略拒绝在指定的时间和天内对所选节点或设备组进行访问。
10. 单击“更新”将新策略添加到 CC-SG，然后在出现的确认消息中单击“是”。

注：如果创建一个策略拒绝（“拒绝”）对节点组或设备组的访问，也必须要创建一个策略允许对所选节点组或设备组的访问（“控制”）。当“拒绝”策略不生效时，用户不会自动获得“控制”权限。

编辑策略

编辑策略时，所做的更改不会影响当前登录到 CC-SG 的用户。更改将在下次登录时生效。如果需要保证更改尽快生效，则先进行维护模式，然后再编辑策略。进入维护模式后，所有当前用户都从 CC-SG 中注销，直到退出维护模式后用户才能再次登录。详情参见**第 11 章：系统维护中的“维护模式”**。

要编辑策略：

1. 从“关联”菜单中，单击“策略”。出现“策略管理器”窗口。
2. 单击“策略名称”下拉箭头，从列表中选择要编辑的策略。
3. 要编辑策略的名称，单击“编辑”。出现“编辑策略”窗口。在字段内键入策略的新名称，然后单击“确认”更改策略的名称。
4. 单击“设备组”下拉箭头，选择此策略管理对其访问的设备组。
   单击“节点组”下拉箭头，选择此策略管理对其访问的节点组。
   如果策略仅覆盖一种类型的组，则仅为该类型选择值。
5. 单击“天”下拉箭头，选择此策略覆盖一周中的哪些天：“全部”（每天）、“工作日”（仅从周一到周五）、“周末”（仅周六和周日）或“自定义”（选择特定天）。
   a. 选择“自定义”可选择自己的天集合。各个天的复选框将被启用。
   b. 对于要此策略覆盖的每一天，选中其对应的复选框。
6. 在“开始时间”字段中，键入此策略开始生效的时间。时间必须是 24 小时格式。
7. 在“结束时间”字段中，键入此策略当天结束的时间。时间必须是 24 小时格式。
8. 在“设备/节点访问权限”字段中，选择“控制”即定义此策略允许在指定的时间和天内对所选节点或设备组进行访问。选择“拒绝”即定义此策略拒绝在指定的时间和天内对所选节点或设备组进行访问。
9. 如果在“设备/节点访问权限”字段中选择“控制”，则会启用“虚拟媒体权限”部分。如果要定义此策略以允许“虚拟媒体权限”，请选择“读写”或“只读”权限。如果要定义此策略以拒绝“虚拟媒体权限”，请选择“拒绝”。
10. 单击“更新”将更改保存到策略，然后在出现的确认消息中单击“是”。

删除策略

要删除策略：

1. 从“关联”菜单中，单击“策略”。出现“策略管理器”窗口。
2. 单击“策略名称”下拉箭头，从列表中选择要删除的策略。
3. 单击“删除”，然后在出现的确认消息中单击“是”。

将策略应用到用户组

策略必须要分配到用户组才会生效。策略被分配到用户组后，组内成员的访问将受到该策略的管理。有关将策略分配到用户组的详细信息，请参见**第 7 章：添加和管理用户和用户组**。

第 9 章：配置远程认证

认证和授权 (AA)

CC-SG 的用户可在 CC-SG 上本地认证和授权，也可使用以下支持的目录服务器进行远程认证：

- Microsoft Active Directory (AD)
- Netscape 的 Lightweight Directory Access Protocol (LDAP)
- TACACS+
- RADIUS

任意数量的远程 RADIUS、TACACS+ 和 LDAP 服务器可用于外部认证。例如，可配置三台 AD 服务器、两台 iPlanet (LDAP) 服务器和三台 RADIUS 服务器。

认证流程

启用远程认证后，认证和授权按照下面的步骤进行：

1. 用户使用合适的用户名和密码登录到 CC-SG。
2. CC-SG 连接到外部服务器并发送用户名和密码。
3. 用户名和密码被接受或拒绝，然后被返回。如果认证被拒绝，则产生失败的登录尝试。
4. 如果认证成功，则执行本地授权。CC-SG 检查所输入的用户名是否匹配在 CC-SG 中创建或从 AD 中导入的组，并按照指定的策略授予权限。

远程被禁用时，认证和授权在 CC-SG 本地完成。

用户帐户

必须将用户帐户添加到认证服务器才能进行远程认证。除了使用 AD 同时进行认证和授权以外，所有远程认证服务器都需要在 CC-SG 上创建用户。用户在认证服务器和 CC-SG 上的用户名必须相同，但密码可以不同。禁用远程认证时仅使用本地 CC-SG 密码。有关添加将被远程认证的用户的详细信息，请参阅**第 7 章：添加和管理用户和用户组**。

***注：**如果使用远程认证，用户必须联系其管理员，在远程服务器上更改其密码。在 CC-SG 上不能为远程认证用户更改密码。*

LDAP 和 AD 专有名称

在 LDAP 或 AD 上配置远程认证用户需要输入用户名，并以“专有名称”的格式搜索。完整的 DN 格式在 **RFC2253** 中予以介绍。对于在本文中的使用，需要了解如何输入专有名称、专有名称各个部分应以何种顺序列出。

为 AD 指定专有名称时应按照此结构，但不是一定要同时指定“公用名”和“组织单位”。

`common name (cn), organizational unit (ou), domain component (dc)`

为 Netscape LDAP 和 eDirectory LDAP 指定 DN 时应按照以下结构：

`user id (uid), organizational unit (ou), organization (o)`

用户名

在“用户名”中指定 **cn=administrator,cn=users,dc=xyz,dc=com** 在 AD 服务器上认证 CC-SG 用户时，如果 CC-SG 与导入的 AD 组关联，则将通过这些凭证授予访问权。注意，可指定多个公用名、组织单位和域组件。

基本 DN

也可输入一个专有名称（DN）来指定从何处开始搜索用户。在“基本 DN”字段中输入一个 DN 即指定查找用户的 AD 容器。例如，输入 **ou=DCAdmins,ou=IT,dc=xyz,dc=com** 将会搜索 **xyz.com** 域下 **DCAdmins** 和 **IT** 组织单位中的所有用户。

AD 配置

将 AD 模块添加到 CC-SG

CC-SG 支持对从 AD 域控制器导入用户的认证和授权，不需要用户在 CC-SG 本地进行定义。这样可允许用户在 AD 服务器上进行专有性的维护。将 AD 服务器配置为 CC-SG 内的模块后，CC-SG 可为给定的域查询所有域控制器。可将 CC-SG 内的 AD 模块与 AD 服务器进行同步，保证 CC-SG 拥有 AD 用户组上最新的授权信息。

重要说明：开始此过程之前，先创建合适的 AD 用户组并为其分配 AD 用户。同时，确保在“配置管理器”中配置了 CC-SG DNS 和域前缀。详情参见**第 12 章：任务管理器****。**

要将 AD 模块添加到 CC-SG：

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕，显示“常规”选项卡。
2. 单击“添加...”打开“添加模块”窗口。

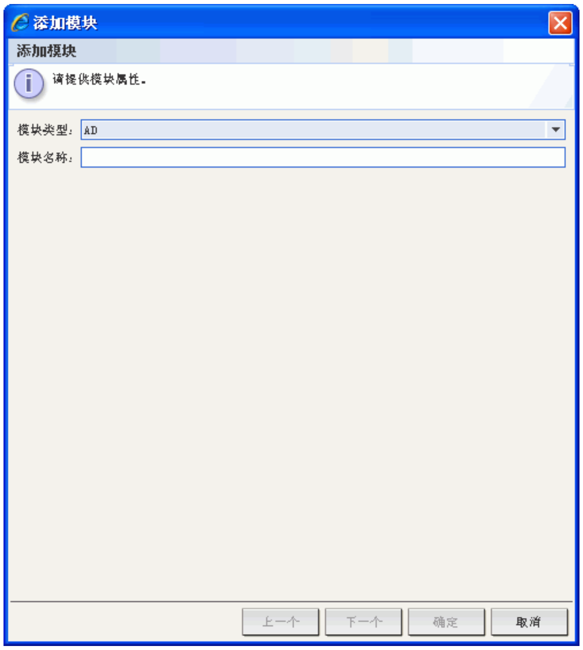


图 95 添加模块

3. 单击“模块类型”下拉菜单，从列表中选择 AD。
4. 在“模块名称”字段中键入 AD 服务器的名称。模块名称是可选的，其指定为了将 AD 服务器模块与 CC-SG 中配置的其它模块区分开来。这个名称不会连接到实际的 AD 服务器名称。
5. 单击“下一步”继续。打开“常规”选项卡

AD 常规设置

在“常规”选项卡内，添加允许 CC-SG 查询 AD 服务器的信息。

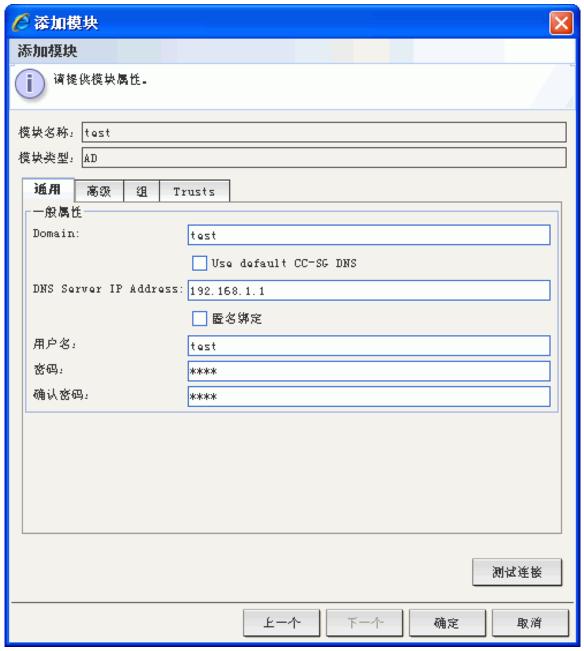


图 96 AD 常规设置

1. 在“域”字段中键入要查询的 AD 域。例如，如果 AD 域安装在 xyz.com 域内，则在“域”字段中键入 xyz.com。CC-SG 以及要查询的 AD 服务器必须在同一个域上配置，或者在彼此信任的不同域上配置。

注：CC-SG 将查询所有已知域控制器，查找所指定的域。

---

2. 在“DNS 服务器 IP 地址”字段中键入 DNS 服务器的 IP 地址。或者，选中“使用默认 CC-SG DNS”复选框使用在 CC-SG 的“配置管理器”部分内配置的 DNS。详情参见第 12 章：任务管理器。
3. 如果想连接 AD 服务器而不指定用户名和密码，则选中“匿名绑定”复选框。如果选中此选项，确保 AD 服务器允许匿名查询。

注：默认情况下， Windows 2003 不允许匿名查询。Windows 2000 服务器允许某些匿名操作，其查询结果基于每个对象的权限。

---

4. 如果不使用匿名绑定，请在“用户名”字段中键入查询 AD 服务器时要使用的用户帐户用户名，格式如下：**username@domain.com**。所指定的用户必须有在 AD 域内执行搜索查询的权限。例如，用户可能属于 AD 内的一个组，其“组范围”设为“全局”且“组类型”设为“安全”。
5. 在“密码”和“确认密码”字段中键入将用于查询 AD 服务器的用户帐户的密码。
6. 单击“测试连接”使用给定的参数测试到 AD 服务器的连接。应收到成功连接的确认。如果没有看到确认，认真检查设置并纠正错误，然后再试。
7. 单击“下一步”继续。打开“高级”选项卡。

AD 高级设置

1. 如果想要配置高级设置，单击“高级”选项卡。

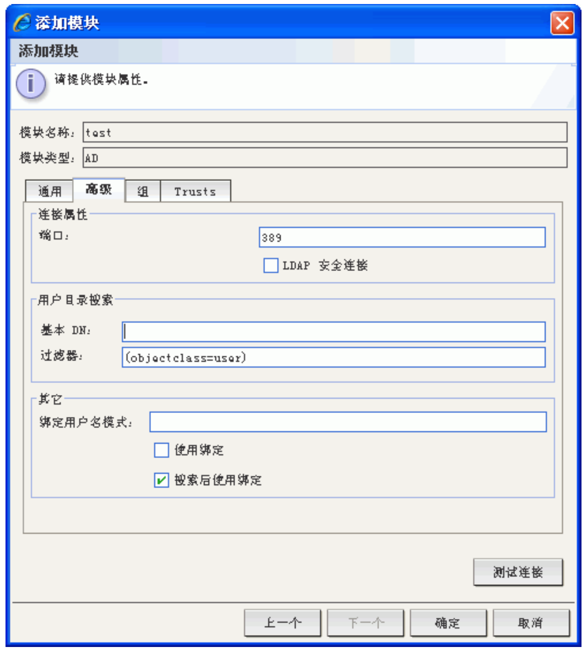


图 97 AD 高级设置

2. 键入 AD 服务器正在监听的端口号。默认端口为 389。如果为 LDAP 使用安全连接（下面第 3 步），则需要更改此端口。安全 LDAP 连接的标准端口为 636。
3. 如果要使用安全通道进行连接，则选中“LDAP 安全连接”。如果选中，则 CC-SG 使用 LDAP over SSL 连接 AD。AD 配置可能不支持此选项。
4. 指定一个要执行认证搜索查询的“基本 DN”（目录级别/条目）。CC-SG 可从这个基本 DN 向下执行递归搜索。

示例	说明
dc=raritan,dc=com	用户条目的搜索查询将在整个目录结构上进行。
cn=Administrators,cn=Users,dc=raritan, dc=com	用户条目的搜索查询将只在 Administors 子目录（条目）上进行。

5. 在“过滤器”中键入用户的属性，使搜索查询仅限制在符合这些标准的条目上。默认过滤器为 objectclass=user，这表示仅搜索“用户”类型的条目。
6. 指定用户条目执行搜索查询的方式。如果选中“使用绑定”，则 CC-SG 尝试使用 Applet 所提供的用户名和密码来直接连接（或绑定）AD。但是，如果在“绑定用户名模式”中指定一个用户名模式，则该模式将与 Applet 所提供的用户名合并，连接 AD 服务器时将使用合并的用户名。
   例如，如果小程序中提供 **cn={0},cn=Users,dc=raritan,dc=com** 和 **TestUser**，则 CC-SG 使用 **cn=TestUser,cn-Users,dc=raritan,dc=com** 来连接 AD 服务器。对于具有在 AD 服务器中执行搜索查询权限的小程序，只有用户从这种小程序中登录时才选中“使用绑定”。

7. 选中“搜索后使用绑定”即使用在“常规”选项卡中指定的用户名和密码来连接 AD 服务器。将在指定的“基本 DN”中搜索条目，核对是否满足指定的过滤标准、属性“samAccountName”是否等于小程序中输入的用户名。然后使用 Applet 提供的用户名和密码尝试第二次连接（或绑定）。第二次绑定保证用户提供正确的密码。
8. 单击“下一步”继续。打开“组”选项卡。

AD 组设置

在“组”选项卡内，可指定要从中导入 AD 用户组的准确位置。

重要说明：必须先指定组设置，然后才能从 AD 中导入组。

1. 单击“组”选项卡。

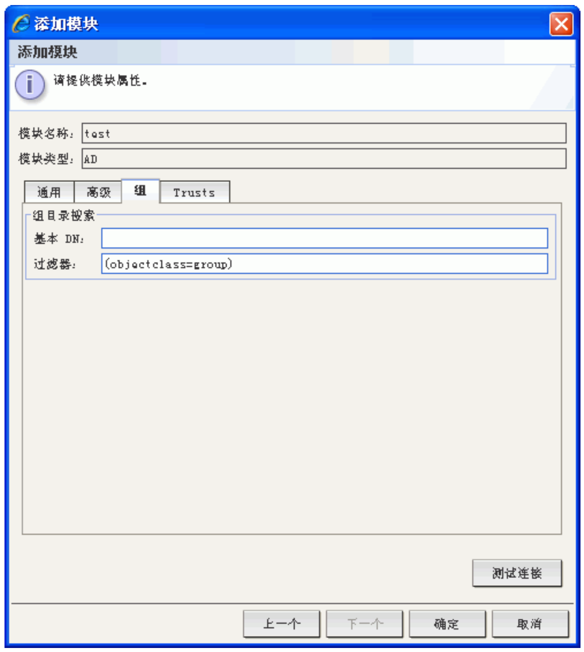


图 98 AD 组设置

2. 指定一个要搜索组（包含待授权的用户）的“基本 DN”（目录级别/条目）。

示例	说明
dc=raritan,dc=com	组内用户的搜索查询将在整个目录结构上进行。
cn=Administrators,cn=Users,dc=raritan, dc=com	组内用户的搜索查询将只在 Administors 子目录（条目）上进行。

3. 在“过滤器”中键入用户的属性，使组内用户的搜索查询仅限制在符合这些标准的条目上。例如，如果为“基本 DN”指定 **cn=Groups,dc=raritan,dc=com**，为“过滤器”指定**(objectclass=group)**，则将返回“组”条目内且类型为“组”的所有条目。
4. 单击“下一步”继续。打开“信任”选项卡。

AD 信任设置

在“信任”选项卡内，可设置新的 AD 域与任何现有域之间的信任关系。信任关系允许认证后的用户跨域访问资源。信任关系可以是入向、出向、双向或禁用。如果想要代表 AD 中不同树系的 AD 模块能够彼此访问信息，则应建立信任关系。

1. 单击“信任”选项卡。如果配置多个 AD 域，则“信任”选项卡将列出所有其它域。

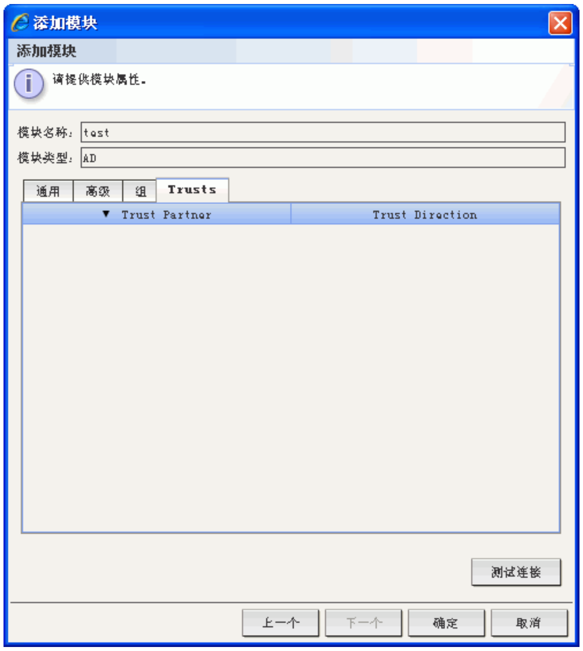


图 99 AD 信任设置

2. 对于“信任伙伴”栏内的每个域，单击“信任方向”下拉菜单，然后选择要在域之间建立的信任方向。对一个 AD 域进行更改时，信任方向将在所有 AD 模块中更新。
   - **入向**：信任从域中过来的信息。在上图中，AD 模块 2 将信任从 AD 模块 1 过来的信息。
   - **出向**：信任到达所选域的信息。在上图中，AD 模块 1 将信任从 AD 模块 2 过来的信息。
   - **双向**：对于每个域信任进出方向的信息。
   - **禁用**：域之间将不进行信息交换。
3. 单击“应用”保存更改，然后单击“确定”保存 AD 模块并退出窗口。

编辑 AD 模块

配置 AD 模块完成后，可随时对其进行编辑。

1. 从“管理”菜单中，单击“安全”。
2. 选择要编辑的 AD 模块，然后单击“编辑”。
3. 在“编辑模块”窗口中单击每个选项卡查看已配置的设置。根据需要进行更改。详情参阅以上小节中的“**AD 常规设置**”、“**AD 高级设置**”、“**AD 组设置**”和“**AD 信任设置**”。
4. 如果更改连接信息，单击“测试连接”使用给定的参数测试到 AD 服务器的连接。应收到成功连接的确认。如果没有看到确认，认真检查设置并纠正错误，然后再试。
5. 单击“确定”保存更改。必须同步所更改的 AD 用户组，或者可同步所有 AD 模块，以同步所有模块中的所有组和用户。详情参阅“**同步 AD 用户组**”和“**同步所有 AD 模块**”。

导入 AD 用户组

必须先在 AD 模块中指定组设置，然后才能从 AD 服务器中导入组。请参阅第 104 页上的“AD 组设置”。对导入的组或用户进行更改后，必须同步所更改的 AD 用户组，或者可同步所有 AD 模块，以同步所有模块中的所有组和用户。详情参阅“**同步 AD 用户组**”和“**同步所有 AD 模块**”。

***注：**确保在“配置管理器”中配置了 CC-SG DNS 和域前缀，然后才能尝试导入 AD 用户组。详情参见**第 12 章：配置管理器**。*

1. 从“管理”菜单中，单击“安全”。
2. 选择要从中导入 AD 用户组的 AD 模块。
3. 单击“导入组...”获取在 AD 服务器上存储的用户组数值列表。如果任何用户组不在 CC-SG 上，可在此将其导入，然后为其分配一个访问策略。
4. 选中要导入到 CC-SG 的组旁边的复选框。单击一个栏标题即按该栏中的信息对用户组列表进行排序。要搜索用户组，在“搜索用户组”字段中键入搜索字符串，然后单击“执行”。单击“全选”选择所有用户组进行导入。单击“取消全选”取消选择所有已选定的用户组。
5. 在“策略”栏内单击字段，然后从列表中选择一个 CC-SG 访问策略，将策略分配到所选的组。这些策略应已经创建，详情参阅第 8 章：策略。
6. 单击“导入”导入所选的用户组。
7. 要检查组是否正确导入并查看刚导入组的权限，单击“用户”选项卡，然后选择导入的组即打开“用户组配置文件”屏幕。单击“权限”和“设备/节点策略”选项卡内的信息。单击“Active Directory 关联”选项卡查看与用户组关联的 AD 模块有关信息。

同步 AD 用户组

同步 AD 用户组时，CC-SG 为所选的 AD 模块检索组、将其名称与已从 AD 导入的用户组进行对比，然后识别匹配。CC-SG 将提供匹配并允许选择要导入哪些组。这可保证 CC-SG 导入最新的 AD 用户组信息。CC-SG 也每天一次自动同步所有 AD 模块。详情参阅下面的“设定 AD 同步时间”。

1. 从“管理”菜单中，单击“安全”。
2. 选择要与 AD 服务器同步的用户组所属的 AD 模块。
3. 单击“同步 AD 用户组”。
4. 当前所选模块中所有导入的用户组都被成功同步后，将出现一条确认消息。

同步所有 AD 模块

当同步所有 AD 模块时，CC-SG 为所有配置的 AD 模块检索用户组、将其名称与已导入到 AD 的用户组进行对比，然后刷新 CC-SG 本地高速缓存。CC-SG 本地高速缓存包含每个域的所有域控制器、所有模块的所有用户组以及已知 AD 用户的用户信息。如果用户组已从 AD 模块中删除，则 CC-SG 也从其本地高速缓存中将其删除。这可保证 CC-SG 有最新的 AD 用户组信息。

1. 必须先进入维护模块，然后才能同步所有 AD 模块。在维护模式中，所有用户都将从 CC-SG 中注销。在“系统维护”菜单中，单击“维护模式”，然后单击“进入维护模式”。
2. 在“进入维护模式”屏幕中，在相应的字段中键入要对从 CC-SG 中注销的用户所显示的消息、CC-SG 进入维护模式之间要经过的分钟数，然后单击“确定”。
3. 单击确认对话框中的“确定”。
4. 当 CC-SG 进入维护模式时，会再出现一条确认消息。单击“确定”。
5. CC-SG 处于维护模式后，在“管理”菜单中单击“安全”。单击“同步所有 AD 模块”。
7. 当所有 AD 模块都被成功同步后，将出现一条确认消息。
8. 要退出维护模式，在“系统维护”菜单中单击“维护模式”，然后单击“退出维护模式”。
9. 在出现的屏幕中单击“确定”。当 CC-SG 退出维护模式时，会再出现一条确认消息。单击“确定”。

设定 AD 同步时间

默认情况下，CC-SG 将在每天的 23:30 同步所有已配置的 AD 模块。可更改这种自动同步发生的时间。

1. 从“管理”菜单中，单击“安全”。
2. 在屏幕底部的“AD 同步时间”字段中，单击上下箭头选择想要 CC-SG 执行所有 AD 模块每天同步的时间。
3. 单击“更新同步时间”保存更改。

AD 配置—从 CC-SG 3.0.2 升级

如果从 CC-SG 3.0.2 升级到 3.1，则必须重新配置 AD 模块，这样 AD 用户才能登录 CC-SG。CC-SG 3.1 需要为每个 AD 模块指定一个 DNS 和域名。这种配置允许 CC-SG 为给定的域查询所有域控制器。

重要说明：升级到 3.1 以后 CC-SG 将仍然处于维护模式。因此，必须使用 CC 超级用户帐户登录来执行此操作。对于从 3.0.2 升级的系统，默认的 CC 超级用户帐户为 ccroot/raritan0。

要重新配置 AD 模块：

1. 从“管理”菜单中，单击“安全”。
2. 选择要编辑的 AD 模块，然后单击“编辑”。
3. 在“常规”选项卡内，在相应的字段中键入 AD 模块的 DNS 和域名。详情参阅“**AD 常规设置**”。
4. 单击“测试连接”使用给定的参数测试到 AD 的连接。应收到成功连接的确认。如果没有看到确认，认真检查设置并纠正错误，然后再试。
5. 单击“确定”保存更改。
6. 如果要配置高级设置、组设置或信任设置，请单击相应的选项卡查看选项。详情参阅以上小节中的“**AD 高级设置**”、“**AD 组设置**”和“**AD 信任设置**”。单击“确定”保存这些选项卡内的更改。
7. 重复这些步骤重复配置所有 AD 模块。
8. 重新配置所有 AD 模块后，可将导入的 AD 用户组与 AD 服务器进行同步。详情参阅“同步 **AD** 用户组”。
9. 同步每个模块 AD 用户组以后，应同步所有 AD 模块。详情参阅“同步所有 **AD** 模块”。取决与 AD 配置，每个域控制器的同步过程最长可能需要 30 秒钟。在同步过程中如果任何域控制器离线，则该过程可能需要更长时间。

*注：请参阅以下小节熟悉 CC-SG 3.1 如何处理 AD 用户组的同步：“同步所有 **AD** 模块”和“设定 **AD** 同步时间”。有关如何生成包含 AD 用户组信息的报告，请参阅**第 10 章：生成报告，AD 用户组报**。*

将 LDAP (Netscape) 模块添加到 CC-SG

启动并输入用户名和密码后，将通过 CC-SG 或直接将查询转发到 LDAP 服务器。如果用户名和密码与 LDAP 目录中的用户名和密码匹配，则用户认证通过。然后将根据 LDAP 服务器上的本地用户组对用户进行授权。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕，显示“常规”选项卡。
2. 单击“添加...”打开“添加模块”窗口。

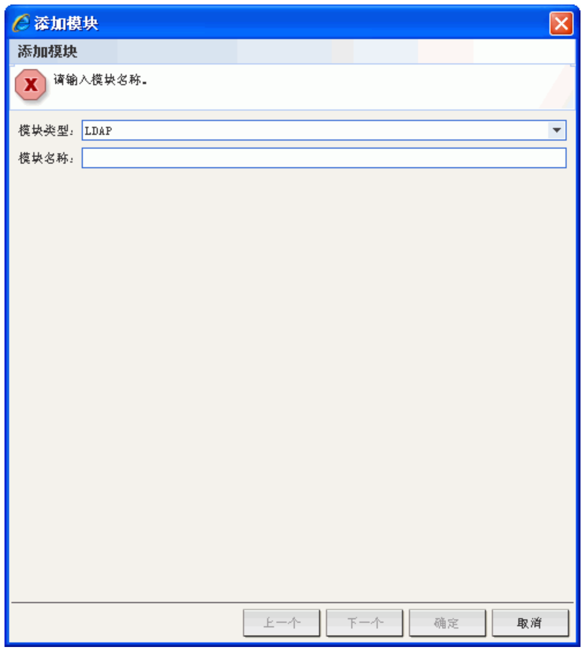


图 100 添加 LDAP 模块

3. 单击“模块类型”下拉菜单，从列表中选择 LDAP。
4. 在“模块名称”字段中键入 LDAP 服务器的名称。
5. 单击“下一步”继续。打开“常规”选项卡。

LDAP 常规设置

1. 单击“常规”选项卡。

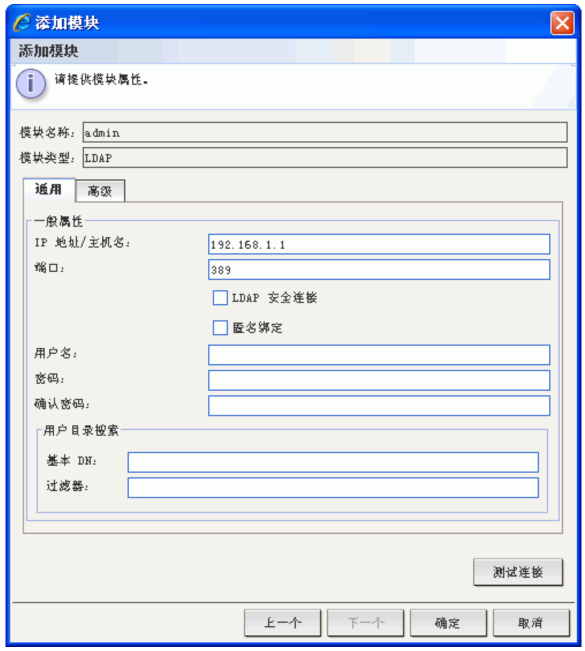


图 101 LDAP 常规设置

2. 在“IP 地址/主机名”字段中键入 LDAP 服务器的 IP 地址或主机名。对于主机名规则，参见**第 1 章：简介**中的“**术语/缩略语**”。
3. 在“端口”字段内键入端口值。默认端口为 389。
4. 如果使用安全 LDAP 服务器，则选中“LDAP 安全连接”。
5. 如果 LDAP 服务器允许匿名查询，则选中“匿名绑定”。对于匿名绑定，不需要输入用户名和密码。

注：默认情况下， Windows 2003 不允许匿名查询。Windows 2000 服务器允许某些匿名操作，其查询结果基于每个对象的权限。

6. 如果不使用匿名绑定，请在“用户名”字段中键入用户名。输入一个专有名称 (DN) 来指定用于查询 LDAP 服务器的凭证。对于 DN，输入公用名、组织单位和域。例如，键入 **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**。使用逗号分割值，但逗号前后不要有空格。值本身可以包含空格，例如 **Command Center**。
7. 在“密码”和“确认密码”字段内键入密码。
8. 要指定从何处开始搜索，在“基本 DN”中输入一个专有名称。例如 **ou=Administrators,ou=TopologyManagement,o=NetscapeRoot** 搜索域下面的所有组织单位。
9. 要将搜索缩小到特殊的对象类型，在“过滤器”字段内键入一个值。例如，**(objectclass=person)** 将搜索缩小到仅人物对象。
10. 单击“测试连接”使用给定的参数测试 LDAP 服务器。应收到成功连接的确认。否则，认真检查设置并纠正错误，然后再试。
11. 单击“下一步”前进到“高级”选项卡，设置 LDAP 服务器的高级配置选项。

LDAP 高级设置

1. 单击“高级”选项卡。

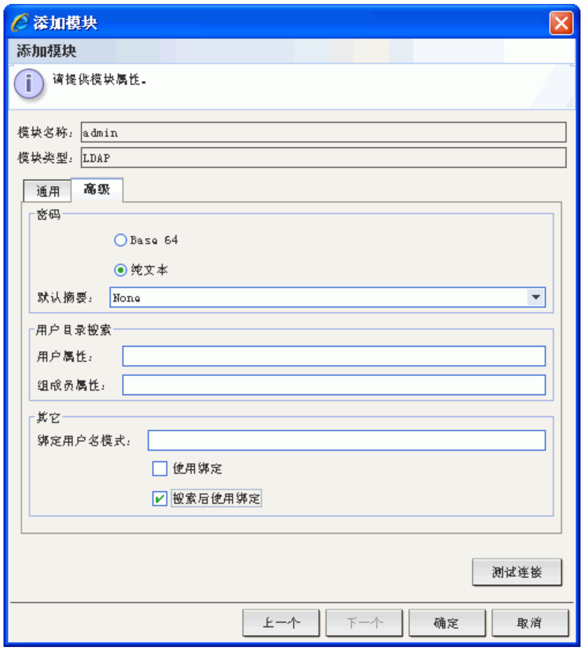


图 102 LDAP 高级设置

2. 如果要使用加密将密码发送到 LDAP 服务器，则单击“Base 64”单选按钮。如果要使用纯文本将密码发送到 LDAP 服务器，则单击“纯文本”单选按钮。
3. 单击“默认 Digest”下拉菜单并选择用户密码的默认加密。
4. 在“用户属性”和“组成员属性”字段中键入用户属性和组成员属性参数。这些值应从 LDAP 目录架构中获得。
5. 在“绑定用户名模式”字段内键入绑定模式。
6. 如果想要 CC-SG 将登录时输入的用户名和密码发送到 LDAP 服务器用于认证，则选中“使用绑定”。如果未选中“使用绑定”，CC-SG 将从 LDAP 服务器中搜索用户名，如果发现，则检索 LDAP 对象，并在本地对比关联的密码与输入的密码。
7. 在有些 LDAP 服务器上，密码不能作为 LDAP 对象的部分进行检索。选中“搜索后使用绑定”即指示 CC-SG 将密码再次绑定到 LDAP 对象，并送回服务器进行认证。
8. 单击“确定”保存更改。

Sun One LDAP (iPlanet) 配置设置

如果使用 Sun One LDAP 服务器进行远程认证，可使用以下参数设置示例：

参数名称	SUN ONE LDAP 参数
IP 地址/主机名	**<Directory Server IP Address>**
用户名	**CN=<Valid user id>**
密码	***<Password>***
基本 **DN**	**O=<Organization>**
过滤器	**(objectclass=person)**
密码（“高级”屏幕）	纯文本
密码默认 **Digest**（高级）	**SHA**
使用绑定	不选中
搜索后使用绑定	选中

OpenLDAP (eDirectory) 配置设置

如果使用 OpenLDAP 服务器进行远程认证，可使用以下示例：

参数名称	OPEN LDAP 参数
IP 地址/主机名	**<Directory Server IP Address>**
用户名	**CN=<Valid user id>, O=<Organization>**
密码	**<Password>**
用户库	**O=accounts, O=<Organization>**
用户过滤器	**(objectclass=person)**
密码（“高级”屏幕）	**Base64**
密码默认 **Digest**（高级）	加密
使用绑定	不选中
搜索后使用绑定	选中

LDAP 证书设置

LDAP 证书设置允许上载 LDAP 证书。可接受或拒绝上载的证书。

1. 单击“高级”选项卡。
2. 单击“浏览”，导航到要上载的证书文件，然后单击“打开”。
3. 单击“接受”接受为 CC-SG 信任的证书。单击“拒绝”删除证书。
4. 如果要删除证书，请选择该证书，然后单击“删除”。
5. 单击“确定”保存更改。

添加 TACACS+ 模块

使用 TACACS+ 服务器进行远程认证的 CC-SG 用户需要在 TACACS+ 服务器上以及 CC-SG 上创建。用户在 TACACS+ 服务器和 CC-SG 上的用户名必须相同，但密码可以不同。有关添加将被远程认证的用户的详细信息，请参阅**第 7 章：添加和管理用户和用户组**。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕，显示“常规”选项卡。
2. 单击“添加...”打开“添加模块”窗口。

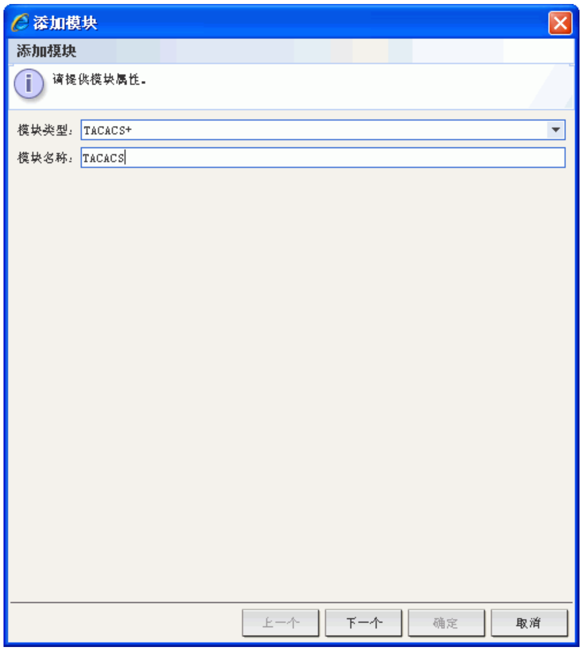


图 103 添加 TACACS+ 模块

3. 单击“模块类型”下拉菜单，从列表中选择 TACACS+。
4. 在“模块名称”字段中键入 TACACS+ 服务器的名称。
5. 单击“下一步”继续。打开“常规”选项卡。

TACACS+ 常规设置

1. 在“IP 地址/主机名”字段中键入 TACACS+ 服务器的 IP 地址或主机名。对于主机名规则，参见第 1 章：简介中的“术语/缩略语”。

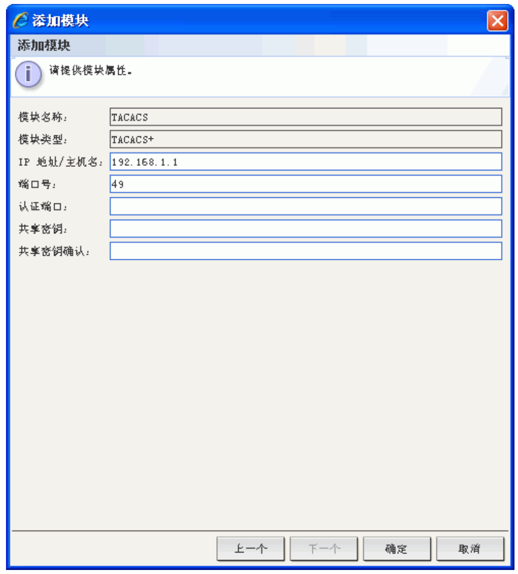


图 104 TACACS+ 常规设置

2. 在“端口号”字段中键入 TACACS+ 服务器正在监听的端口号。默认端口号为 **49**。
3. 在“认证端口”字段内键入认证端口。
4. 在“共享密钥”和“共享密钥确认”字段中键入共享密钥。
5. 单击“确定”保存更改。

添加 RADIUS 模块

使用 RADIUS 服务器远程认证的 CC-SG 用户需要在 RADIUS 服务器上以及 CC-SG 上创建。用户在 RADIUS 服务器和 CC-SG 上的用户名必须相同，但密码可以不同。有关添加将被远程认证的用户的详细信息，请参阅**第 7 章：添加和管理用户和用户组**。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕，显示“常规”选项卡。
2. 单击“添加...”打开“添加模块”窗口。

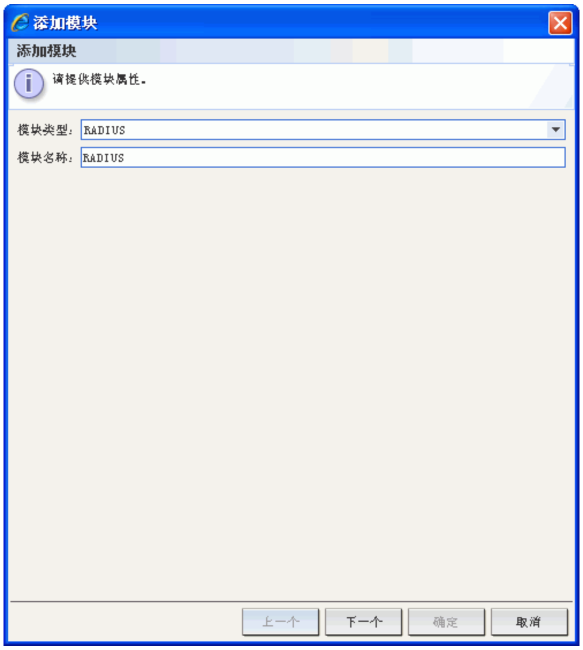


图 105 安全管理器添加模块屏幕

3. 单击“模块类型”下拉菜单，从列表中选择 RADIUS。
4. 在“模块名称”字段中键入 RADIUS 服务器的名称。
5. 单击“下一步”继续。打开“常规”选项卡。

RADIUS 常规设置

1. 单击“常规”选项卡。



图 106 指定 RADIUS 服务器

2. 在“IP 地址/主机名”字段中键入 RADIUS 服务器的 IP 地址或主机名。对于主机名规则，参见**第 1 章：简介**中的**“术语/缩略语”**。
3. 在“端口号”字段内键入端口号。默认端口号为 1812。
4. 在“认证端口”字段内键入认证端口。
5. 在“共享密钥”和“共享密钥确认”字段中键入共享密钥。
6. 单击“确定”保存更改。

使用 RADIUS 的双因素认证

通过将支持双因素认证的 RSA RADIUS 服务器联合 RSA 认证管理器一起使用，CC-SG 可通过动态令牌使用双因素认证方案。

在这种环境中，用户登录 CC-SG 时首先要在“用户名”字段中键入其用户名。然后在“密码”字段中键入其固定密码，后跟动态的令牌值。

用于启用这种方式的 RADIUS 服务器和认证管理器的配置不在本文涵盖范围之内。CC-SG 的配置与上述标准 RADIUS 远程认证的配置相同。CC-SG 应配置为指向 RADIUS 服务器。详情参阅**附录 G：双因素认证**。

指定认证和授权模块

将所有外部服务器添加为 CC-SG 内的模块以后，可指定是否要 CC-SG 使用各个模块进行认证、授权或同时两项功能。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕时，单击“常规”选项卡。所有已配置的外部认证和授权服务器显示在“外部 AA 服务器”部分内。
2. 对于每一台服务器，如果想要 CC-SG 使用该服务器进行用户认证，则选中“认证”复选框。
3. 对于每一台服务器，如果想要 CC-SG 使用该服务器进行用户授权，则选中“授权”复选框。只有 AD 服务器能用于授权。
4. 单击“更新”保存更改。

建立外部 AA 服务器的顺序

在“常规”选项卡内，可设定 CC-SG 查询已配置外部 AA 服务器时的顺序。如果第一个选中的选项不可用，则 CC-SG 将尝试第二个，然后第三个，以此类推，直到失败。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕时，单击“常规”选项卡。

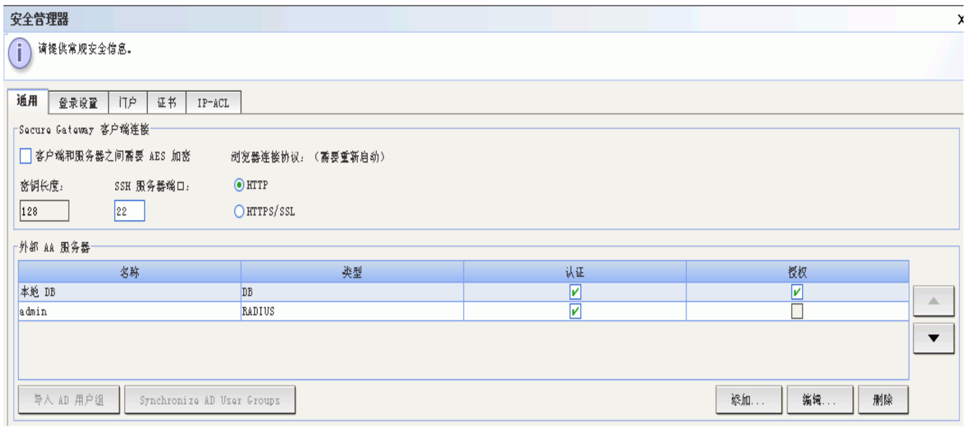


图 107 安全管理器常规选项卡

2. “外部 AA 服务器”部分列出 CC-SG 中所有可用的认证和授权选项。从列表中选择一个名称，单击上下箭头排列使用的优先顺序。
3. 单击“更新”保存更改。

此页专门留白。

第 10 章：生成报告

单击栏标题可对报告进行排序。单击一个栏标题即按该栏内的值对报告数据进行排序。将按照字母升序、数字升序或时间先后顺序刷新数据。再次单击该栏标题即按降序排列。

所有报告中的栏宽度都可以调整大小。将鼠标指针放置在标题行内的栏分割线上，直到指针形状变成双向箭头。单击并左右拖动鼠标即可调节栏的宽度。

所使用的排序值和栏宽度将在下次登录和运行 CC-SG 报告时成为默认报告视图。对于所有报告，双击一行即可查看报告的详细信息。

注：在所有报告中，使用 Ctrl 键单击鼠标可取消选择选中的行。

审计跟踪报告

“审计跟踪”报告显示 CC-SG 内的审计日志和访问。它捕获添加、编辑或删除设备或端口的操作，以及其它修改。

CC-SG 维护以下事件的“审计跟踪”：

- CC-SG 启动
- CC-SG 停止
- 用户登录 CC-SG
- 用户注销 CC-SG
- 用户开始节点连接

1. 在“报告”菜单上，单击“审计跟踪”。出现“审计跟踪”屏幕。



图 108 审计跟踪屏幕

2. 在“开始日期”和“结束日期”字段内设定报告的日期范围。单击默认日期（月、日、年、时、分、秒）的每个部分进行选择，然后单击上下箭头调到所需的数字。
3. 通过在“消息”、“用户名”和“用户 IP 地址”字段中输入附加参数，可限制报告中将要包含的数据。

- 如果要按照与活动关联的消息文本限制报告，请在“消息”字段中键入文本。
- 如果要将报告限制为特殊用户的活动，请在“用户名”字段中键入该用户的用户名。
- 如果要将报告限制为特殊 IP 地址的活动，请在“用户 IP 地址”字段中键入该用户的 IP 地址。

4. 单击“确定”运行报告。将生成报告，显示在指定的时间周期内发生的、符合任何所指定的附加参数的活动有关数据。

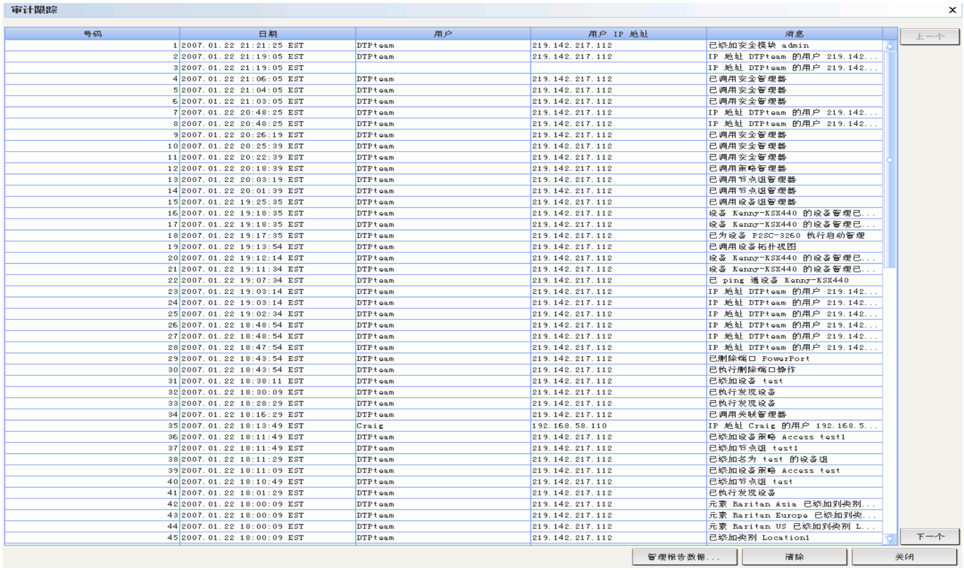


图 109 审计跟踪报告

- 单击“下一页”或“上一页”在报告页面之间导航。
- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“清除”即清除报告中使用的日志文件。
- 单击“关闭”关闭报告。

错误日志报告

CC-SG 在一系列的“错误日志”文件中存储错误消息，可访问这些日志帮助排除问题。

1. 在“报告”菜单上，单击“错误日志”。出现“错误日志”屏幕。

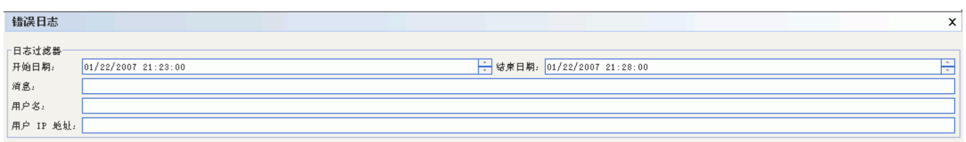


图 110 错误日志屏幕

2. 在“开始日期”和“结束日期”字段内设定报告的日期范围。单击默认日期（月、日、年、时、分、秒）的每个部分进行选择，然后单击上下箭头调到所需的数字。
3. 通过在“消息”、“用户名”和“用户 IP 地址”字段中输入附加参数，可限制报告中将要包含的数据。

- 如果要按照与活动关联的消息文本限制报告，请在“消息”字段中键入文本。
- 如果要将报告限制为特殊用户的活动，请在“用户名”字段中键入该用户的用户名。
- 如果要将报告限制为特殊 IP 地址的活动，请在“用户 IP 地址”字段中键入该用户的 IP 地址。

4. 单击“确定”运行报告。将生成报告，显示在指定的时间周期内发生的、符合任何所指定的附加参数的活动有关数据。

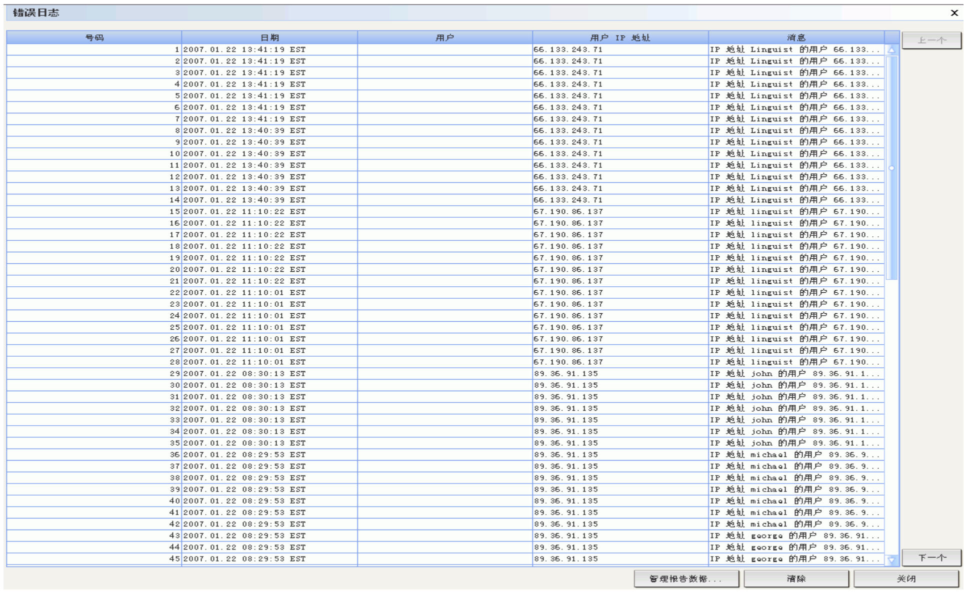


图 111 错误日志报告

- 单击“下一页”或“上一页”在报告页面之间导航。
- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“清除”即清除报告中使用的日志文件。
- 单击“关闭”关闭报告。

访问报告

运行“访问”报告即可查看任何访问的设备和端口、访问的时间以及访问的用户相关信息。

1. 在“报告”菜单上，单击“访问报告”。出现“访问报告”屏幕。

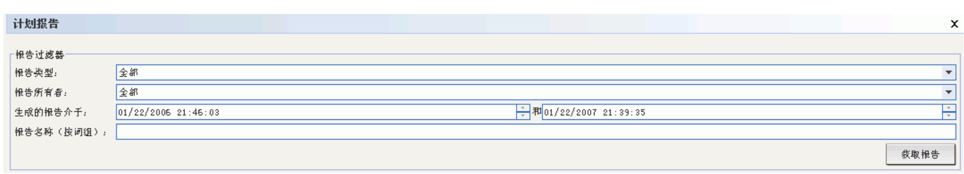


图 112 访问报告屏幕

2. 在“开始日期”和“结束日期”字段内设定报告的日期范围。单击默认日期（月、日、年、时、分、秒）的每个部分进行选择，然后单击上下箭头调到所需的数字。
3. 通过在“消息”、“设备名称”、“端口名称”“用户名”和“用户 IP 地址”字段中输入附加参数，可限制报告中将要包含的数据。

- 如果要按照与活动关联的消息文本限制报告，请在“消息”字段中键入文本。
- 如果要将报告限制为特殊设备，请在“设备名称”字段中键入设备名称。
- 如果要将报告限制为特殊端口，请在“端口名称”字段中键入端口名称。
- 如果要将报告限制为特殊用户的活动，请在“用户名”字段中键入该用户的用户名。

- 如果要将报告限制为特殊 IP 地址的活动，请在“用户 IP 地址”字段中键入该用户的 IP 地址。

4. 单击“确定”运行报告。将生成报告，显示在指定的时间周期内发生的、符合任何所指定的附加参数的访问有关数据。

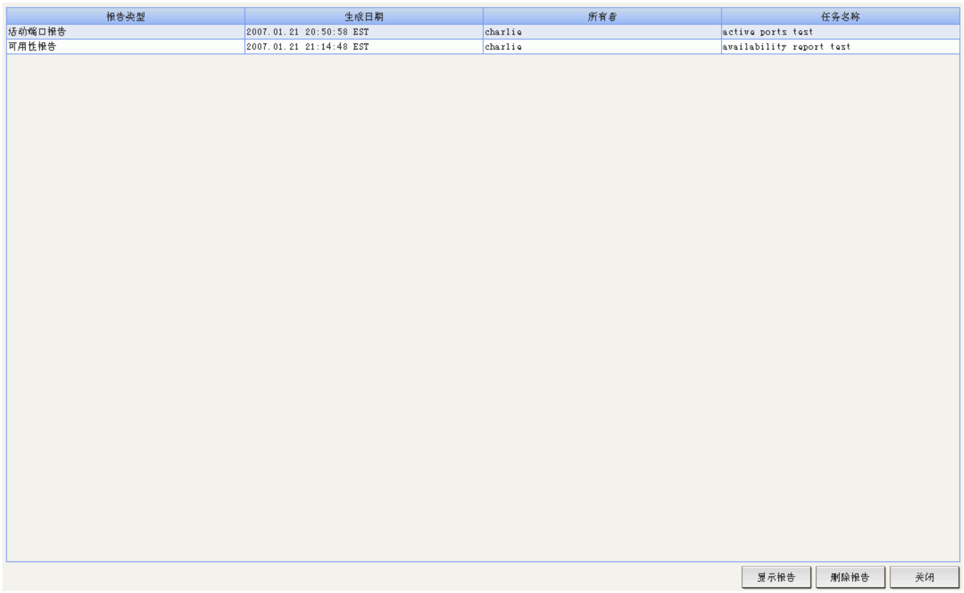


图 113 访问报告

- 单击“下一页”或“上一页”在报告页面之间导航。
- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“清除”即清除报告中使用的日志文件。
- 单击“关闭”关闭报告。

可用性报告

“可用性报告”显示所有连接的状态，按名称和 IP 地址显示设备。此报告提供系统上设备的完整的可访问性图形，所提供的信息可帮助进行故障排除。

1. 在“报告”菜单上，单击“可用性报告”。生成“可用性报告”。

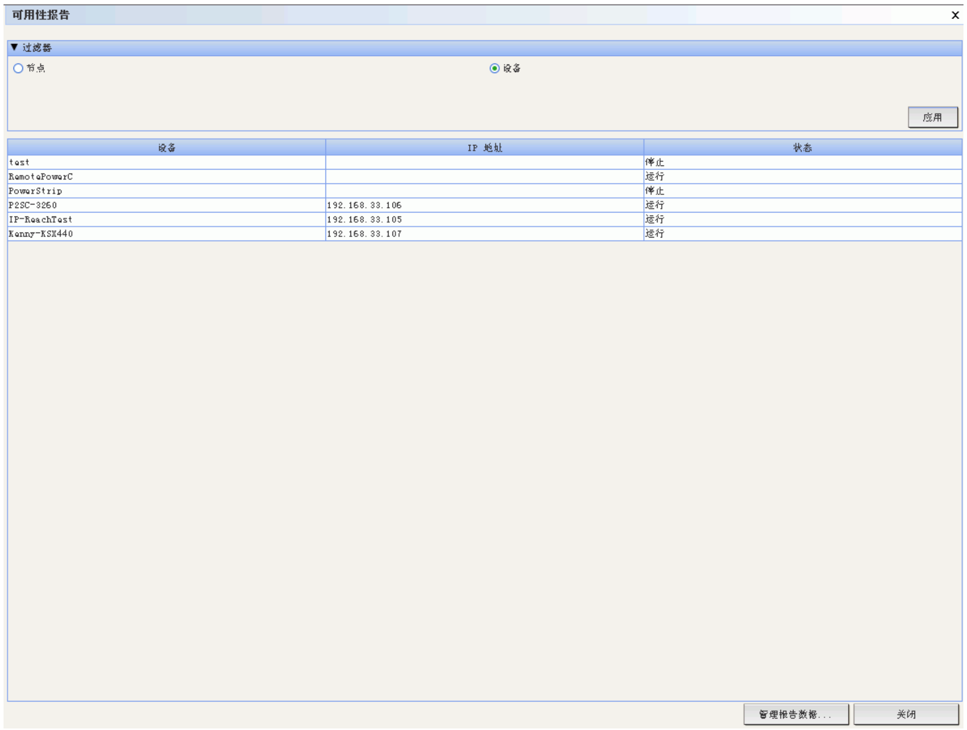


图 114 可用性报告

- 单击“管理报告数据…”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

活动用户报告

“活动用户”报告显示当前用户和用户会话。可从报告中选择活动用户，并将其从 CC-SG 中断开连接。

1. 在“报告”菜单上，单击“用户”，然后单击“活动用户”。生成“活动用户”报告。

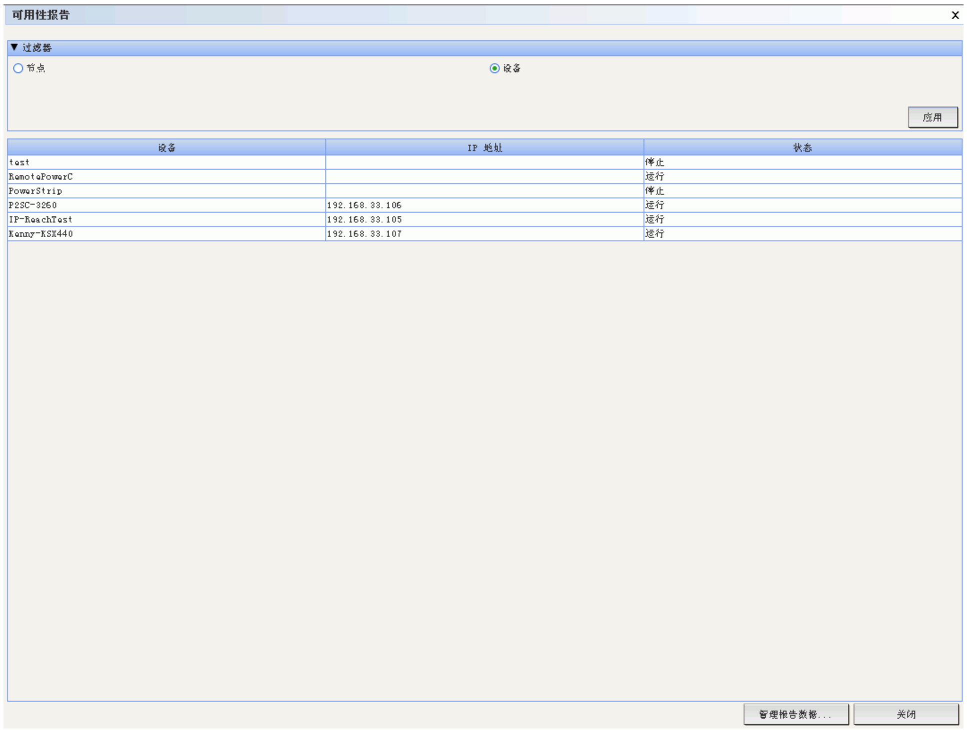


图 115 活动用户报告

- 要将用户从 CC-SG 内的活动会话中断开连接，选择要断开连接的用户名，然后单击“注销”。
- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

锁定用户报告

“锁定用户”报告显示当前因为过多失败登录尝试而被 CC-SG 锁定的用户。可从此报告中解锁用户。有关锁定设置的详细信息，参见第 12 章：高级管理，锁定设置。

1. 在“报告”菜单上，单击“用户”，然后单击“锁定用户”。



锁定报告

锁定的用户

用户	最后已知的 IP 地址	锁定开始	锁定结束
Christian	192.168.50.35	2007-01-24 11:43:34.164	
JackC	192.168.50.51	2007-01-23 17:45:11.207	

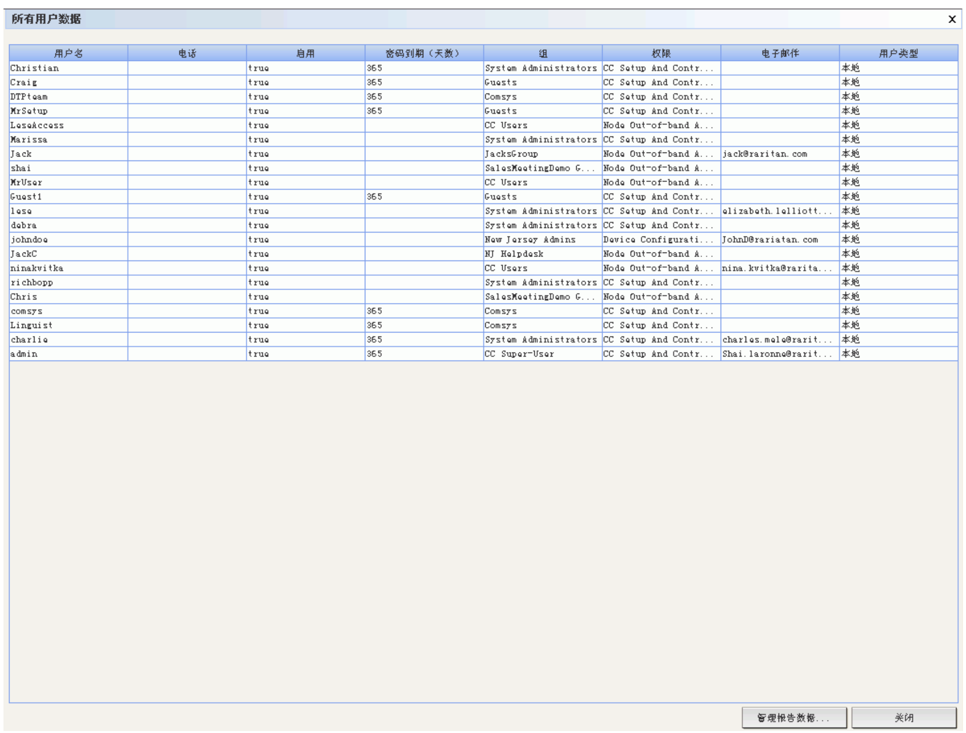
图 116 锁定用户报告

- 要解锁被 CC-SG 锁定的用户，选择要解锁的用户名，然后单击“解锁用户”。
- 单击“取消”关闭报告。

用户数据报告

“用户数据”报告显示 CC-SG 数据库内所有用户的某些数据。

1. 在“报告”菜单上，单击“用户”，然后单击“用户数据”。生成“所有用户数据”报告。



所有用户数据

用户名	电话	启用	密码到期（天数）	组	权限	电子邮件	用户类型
Christian		true	365	System Administrators	CC Setup And Contr...		本地
Craig		true	365	Guests	CC Setup And Contr...		本地
DTPteam		true	365	Comsys	CC Setup And Contr...		本地
MrSetup		true	365	Guests	CC Setup And Contr...		本地
LeseAccess		true		CC Users	Node Out-of-band A...		本地
Marissa		true		System Administrators	CC Setup And Contr...		本地
Jack		true		JacksGroup	Node Out-of-band A...	jack@raritan.com	本地
shai		true		SalesMeetingDemo G...	Node Out-of-band A...		本地
MrUser		true		CC Users	Node Out-of-band A...		本地
Guest1		true	365	Guests	CC Setup And Contr...		本地
lese		true		System Administrators	CC Setup And Contr...	elizabeth.lelliott...	本地
debra		true		System Administrators	CC Setup And Contr...		本地
johndoe		true		New Jersey Admins	Device Configurati...	JohnD@rariatan.com	本地
JackC		true		NJ Helpdesk	Node Out-of-band A...		本地
ninakvitka		true		CC Users	Node Out-of-band A...	nina.kvitka@rarita...	本地
richbopp		true		System Administrators	CC Setup And Contr...		本地
Chris		true		SalesMeetingDemo G...	Node Out-of-band A...		本地
comsys		true	365	Comsys	CC Setup And Contr...		本地
Linguist		true	365	Comsys	CC Setup And Contr...		本地
charlie		true	365	System Administrators	CC Setup And Contr...	charles.mele@rarit...	本地
admin		true	365	CC Super-User	CC Setup And Contr...	Shai.laronne@rarit...	本地

图 117 所有用户数据报告

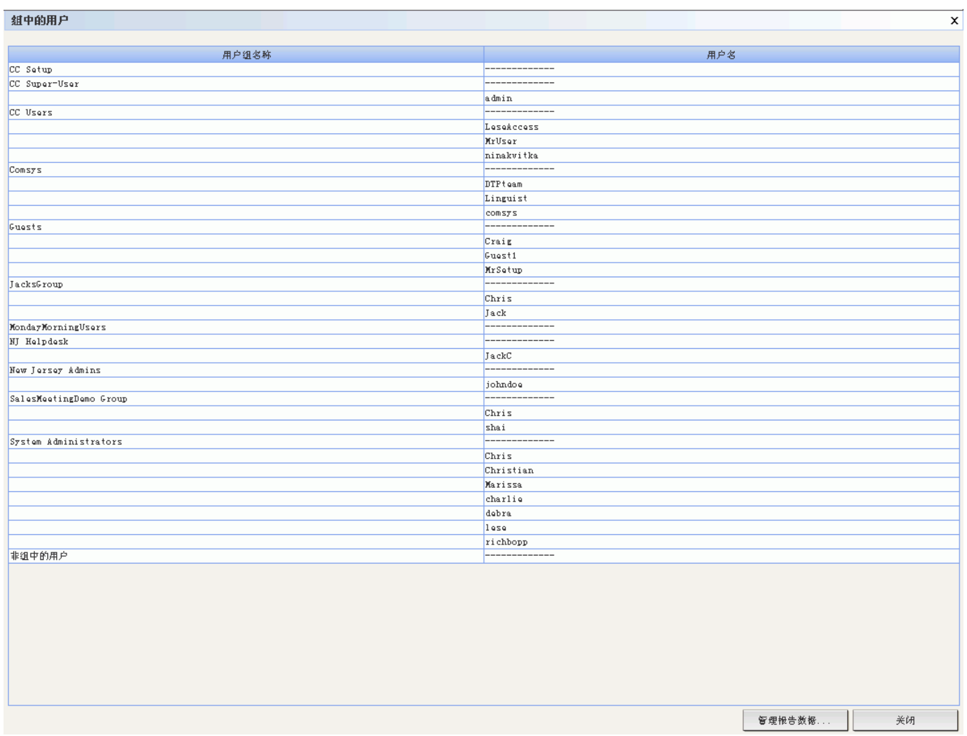
- “用户名称”字段中显示所有 CC-SG 用户的用户名称。
- “电话”字段显示用户的回拨电话号码，仅适用于带有调制解调器的 CC-SG G1 系统用户。

- 如果用户能够登录 CC-SG，则“启用”字段显示为“true”，否则显示为“false”，基于在“用户配置文件”中“登录已启用”复选框是否被选中。详情参见第 7 章：添加和管理用户和用户组，添加用户。
- “密码过期”字段中显示用户可使用相同密码的天数，此天数过后必须更改密码。详情参见第 7 章：添加和管理用户和用户组，添加用户。
- “组”字段显示用户隶属的用户组。
- “权限”字段显示分配给用户的 CC-SG 权限。详情参阅附录 D：SNMP 陷阱。
- “电子邮件”字段显示在“用户配置文件”中指定的用户的电子邮件地址。
- “用户类型”字段显示为“本地”或“远程”，取决于用户的访问方法。
- 单击“管理报告数据…”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

组中的用户报告

“组中的用户”报告显示用户及其关联组的数据。

1. 在“报告”菜单上，单击“用户”，然后单击“组中的用户”。生成“组中的用户”报告。



用户组名称	用户名
CC Setup	------------
CC Super-User	------------
	admin
CC Users	------------
	LoseAccess
	MrUser
	ninakvitka
Comsys	------------
	DTPteam
	Linguist
	comsys
Guests	------------
	Craig
	Guest1
	MrSetup
JacksGroup	------------
	Chris
	Jack
MondayMorningUsers	------------
NJ Helpdesk	------------
	JackC
New Jersey Admins	------------
	johndoe
SalesMeetingDemo Group	------------
	Chris
	shai
System Administrators	------------
	Chris
	Christian
	Marissa
	charlie
	debra
	lese
	richbopp
非组中的用户	------------

图 118 组中的用户报告

- 单击“管理报告数据…”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

组数据报告

“组数据”报告显示用户组、节点组和设备组信息。在一个屏幕上即可按名称和说明查看用户组、按名称查看节点组、按名称查看设备组。

1. 在“报告”菜单上，单击“用户”，然后单击“组数据”。生成“组”报告。

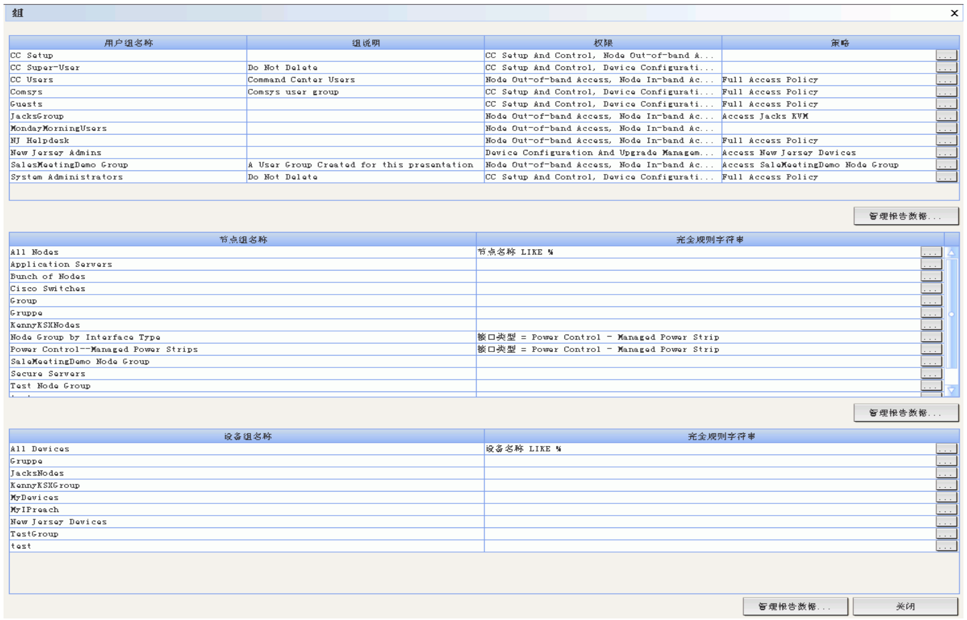


图 119 组报告

- 单击“管理报告数据...”可保存或打印报告部分。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。
- 单击一个行旁边的“...”按钮即可显示与用户组关联的策略，或满足端口组规则的节点列表，或满足设备组规则的设备列表。

AD 用户组报告

“AD 用户组”报告显示从已配置用于认证和授权的 Active Directory 服务器导入到 CC-SG 的组内的所有用户。报告中不含在本地通过 CC-SG 添加到 AD 用户组的用户。

1. 在“报告”菜单上，单击“用户”，然后单击“AD 用户组报告”。出现“AD 用户组报告”屏幕。
2. “AD 服务器”列表包括在 CC-SG 上配置的用于认证和授权的所有 AD 服务器。对于想要 CC-SG 在报告中包括的 AD 服务器，选中其对应的复选框。
3. 在“AD 用户组”部分内，“可用”列表包括从在“AD 服务器”列表中选中的 AD 服务器导入到 CC-SG 中的所有用户组。选择报告中要包括的用户组，然后单击“添加”其移到“已选定”列表。
4. 单击“应用”。生成“AD 用户组”报告。

- 单击“管理报告数据...”可保存或打印报告部分。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

资产管理报告

“资产管理”报告显示当前被 CC-SG 管理的设备上的数据。

1. 在“报告”菜单上，单击“设备”，然后单击“资产管理报告”。将为所有设备生成“资产管理”报告。
2. 如果按设备类型过滤报告数据，请单击“设备类型”下拉箭头，从列表中选择设备类型，然后单击“应用”。将应用所选的过滤器重新生成报告。



图 120 资产管理报告

- 版本不符合“兼容性矩阵”的设备将在“设备名称”字段中用红色文字显示。
- 单击“管理报告数据...”可保存或打印报告部分。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“刷新”生成新的报告。根据系统配置的大小，报告生成可能需要几分钟的时间。
- 单击“关闭”关闭报告。

节点资产报告

“字节资产”报告为 CC-SG 管理之下的所有节点显示节点名称、接口名称和类型、设备名称和类型以及节点组。也可以过滤报告仅包含与指定节点组、接口类型、设备类型或设备对应的节点的数据。

1. 在“报告”菜单上，单击“节点”，然后单击“节点资产报告”。显示“节点资产报告”屏幕。

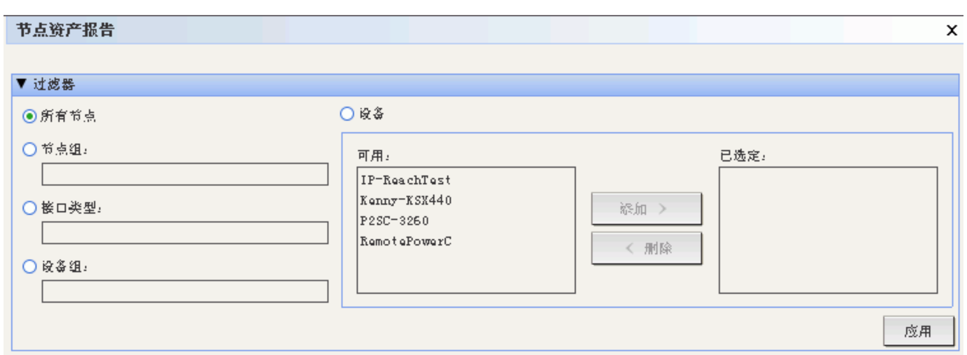


图 121 节点资产报告屏幕

2. 单击要应用到报告的过滤标准所对应的单选按钮：“所有节点”、“节点组”、“设备组”或“设备”。
   - 如果选择“节点组”、“接口类型”或“设备组”，请单击相应的下拉箭头，然后从列表中选择一个参数。
   - 如果选择“设备”，在“可用”列表中选择报告中要包含的节点资产，然后单击“添加”将其移到“已选定”列表中。
3. 单击“应用”生成报告。生成“节点资产”报告。



图 122 节点资产报告

- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

活动节点报告

“活动节点”报告对于具有活动连接的每个节点，包括每个活动接口的名称和类型、当前用户、时间戳以及用户 IP 地址。从此报告中可查看活动节点列表和断开节点连接。

1. 在“报告”菜单上，单击“节点”，然后单击“活动节点”。如果当前有活动节点，则生成“活动节点”报告。

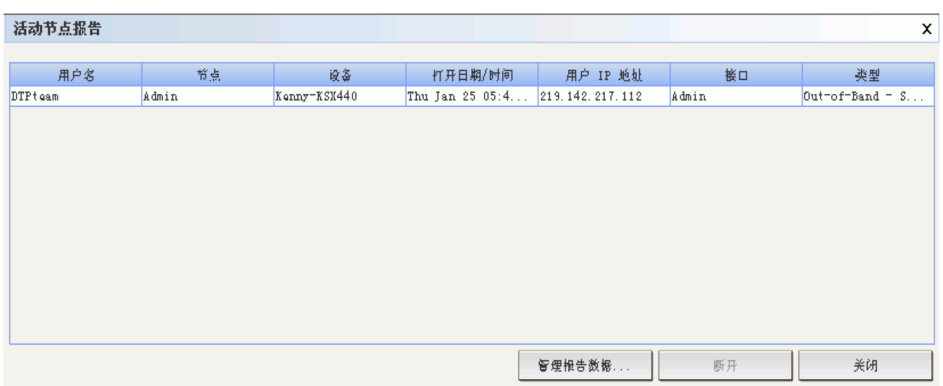


图 123 活动节点报告

- 要从当前会话中断开节点连接，请选择要断开连接的节点，然后单击“断开连接”。
- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

节点创建报告

“节点创建”报告列出在指定的时间框架内所有的节点创建尝试，包括成功的和不成功的创建。可指定是要查看所有的节点创建尝试，还是仅查看潜在重复的节点。

1. 在“报告”菜单上，单击“节点”，然后单击“节点创建”。显示“节点创建”屏幕。



图 124 节点创建报告屏幕

2. 在“开始日期”和“结束日期”字段内设定报告的日期范围。单击默认日期（月、日、年、时、分、秒）的每个部分进行选择，然后单击上下箭头调到所需的数字。
3. 选中“仅潜在重复”复选框将报告限制为那些被标记为潜在重复的节点。
4. 单击“应用”。生成“节点创建”报告。



图 125 节点创建报告

- “结果”字段中显示“成功”、“失败”或“潜在重复”，描述节点创建尝试的结果。
- 单击“管理报告数据...”可保存或打印报告部分。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

查询端口报告

“查询端口”报告根据端口状态显示所有端口。

1. 在“报告”菜单上，单击“端口”，然后单击“查询端口”。出现“查询端口”屏幕。

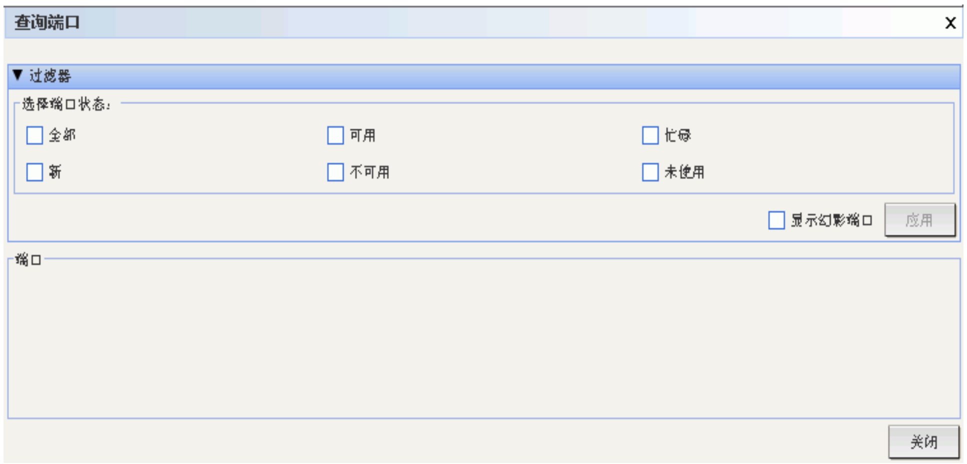


图 126 查询端口屏幕

2. 在“选择端口状态”部分内，选中报告中要包含的端口状态所对应的复选框。选中多个复选框并单击“应用”，将显示所选状态的端口。

端口状态	定义
全部	所有端口状态
新建	端口可用（到目标服务器的物理连接已存在），但端口尚未配置。
未使用	端口不可用（到目标服务器的物理连接不存在），且端口尚未配置。
可用	端口已经配置，可连接端口。
不可用	由于设备关闭或不可用，不能连接端口。
忙碌	用户已经连接到此端口。

3. 选中“显示幻影端口”复选框以及一个或多个端口状态，即显示“幻影的”以及所选状态的端口。当 CIM 或目标服务器从 Paragon 系统中删除或关闭（手动或意外关闭）时，即会出现幻影端口。详情参见 Raritan 的《Paragon II 用户手册》。

4. 单击“应用”生成报告。

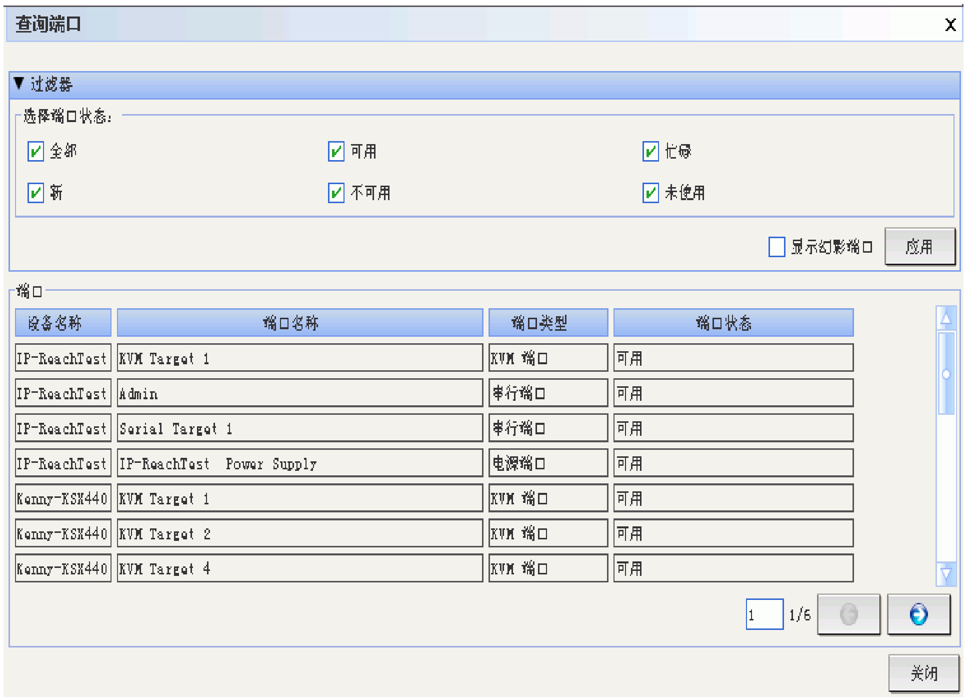


图 127 查询端口报告

- 单击报告底部右侧的箭头图标，可在多页报告中导航。
- 在报告中，单击“新建”或“未使用”端口旁边的“配置”即可进行配置。
- 单击“关闭”关闭报告。

活动端口报告

“活动端口”报告显示当前在用的带外端口。从此报告中可查看活动端口列表和断开端口连接。

1. 在“报告”菜单上，单击“端口”，然后单击“活动端口”。生成“活动端口”报告。

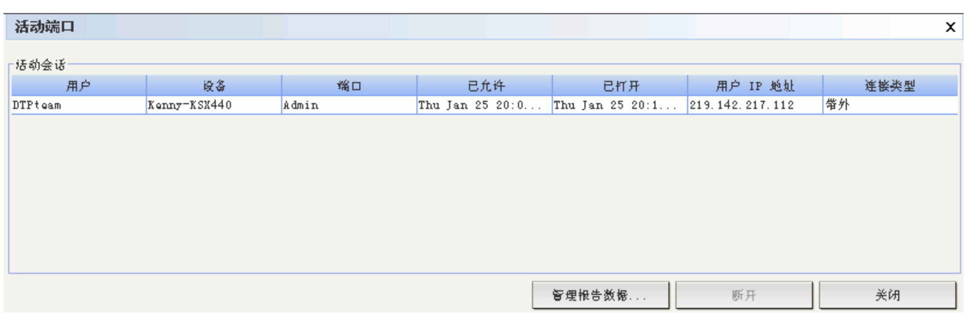


图 128 活动端口报告

- 要从当前会话中断开端口连接，请选择要断开连接的端口，然后单击“断开连接”。
- 单击“管理报告数据...”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。
- 单击“关闭”关闭报告。

计划报告

“计划报告”显示在任务管理器中计划的报告。所有计划报告可用 HTML 格式查看。详情参阅**第 12 章：高级管理**。

1. 在“报告”菜单上，单击“计划报告”。
2. 单击“获取报告”即查看全部所有者创建的所有计划报告的完整列表。默认情况下，显示一小时前计划到当前时间的所有报告。
3. 要过滤所显示的报告，可选择特殊的“报告类型”（例如“活动端口报告”），或选择“报告所有者”，或单击默认日期每个部分（月、日、年、时、分、秒）选择然后单击上下箭头达到所需的数字，从而更改“生成的报告介于”的开始和结束日期。可输入“报告名称”按名称过滤——输入名称的短语或部分短语；匹配时区分大小写，不允许通配符。
4. 单击“获取报告”查看过滤的列表。
5. 要查看单个报告，在列表中选中该报告，然后单击“显示报告”。
6. 单击“关闭”关闭报告。

CC-NOC 同步报告

“CC-NOC 同步”报告列出 CC-SG 订阅的、在给定的特殊发现日期受到 CC-NOC 监视的所有目标及其 IP 地址。此处也显示在配置的范围内发现的任何新目标。详情参阅**第 12 章：高级管理**中的**“添加 CC-NOC”**。可在此报告中清理 CC-SG 数据库中的目标。

1. 在“报告”菜单上，单击“CC-NOC 同步”。
2. 选择“最后发现日期”，然后单击“获得目标”。在“最后发现日期”或在此以前发现的目标显示在“目标已发现”下面。

- 如果要从 CC-SG 数据库内清除目标，请选择要清除的目标，然后单击“清理”。
- 如果要从 CC-SG 数据库内清除整个目标列表，请单击“全部清理”。
- 单击“管理报告数据…”可保存或打印报告。单击“保存”将当前报告页中显示的记录保存为 CSV 文件，或单击“全部保存”保存所有记录。单击“打印”打印当前报告页中显示的记录，或单击“全部打印”打印所有记录。单击“关闭”关闭窗口。

此页专门留白。

第 11 章：系统维护

维护模式

这种模式限制到 CC-SG 的访问，使管理员能够不中断地执行各种操作。可从 GUI 或通过客户端的 SSH 命令行界面执行操作，例如 Putty、OpenSSH 客户端等。详情参见**第12章：高级管理**的“SSH 访问”。

当前用户（发起维护模式的管理员除外）将收到提示，并在可配置的时间周期后注销。在维护模式下，其他管理员可登录 CC-SG，但非管理员禁止登录。每次 CC-SG 进入或退出维护模式时都生成一个 SNMP 陷阱。

注：维护模式仅在单机 CC-SG 设备上可用，在群集配置中不可用。只有在维护模式中才能升级 CC-SG。

计划任务和维护模式

CC-SG 处于维护模式时无法执行计划任务。有关计划任务的详细信息，参见**第 12 章：高级管理，任务管理器**。CC-SG 退出维护模式时，将会尽快执行计划任务。

进入维护模式

要进入维护模式：

1. 在“系统维护”菜单中，单击“维护模式”，然后单击“进入维护模式”。

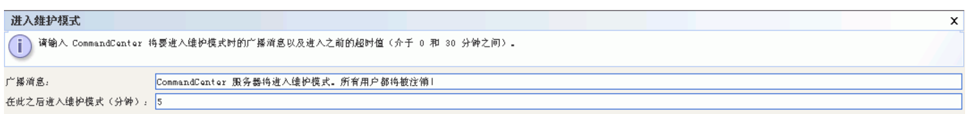


图 129 进入维护模式

2. 键入“广播消息”，或接受所提供的默认广播消息。这条消息将向所有已登录的用户显示，警告 CC-SG 一旦进入维护模式他们将被注销。
3. 在“在此之后进入维护模式（分钟）”字段中输入时间（分钟）。这是 CC-SG 进入维护模式之前的等待时间。此时间可在 0 到 30 分钟之间。时间为 0 则表示立即启动维护模式。
4. 单击“确定”。

退出维护模式

要退出维护模式：

1. 从“系统维护”菜单中，单击“维护模式”。
2. 单击“退出维护模式”。出现“退出维护模式”屏幕。
3. 单击“确定”退出维护模式。

出现一条消息指示 CC-SG 已退出维护模式。所有用户将能够正常访问 CC-SG。

备份 CC-SG

备份 CC-SG 之前先进入维护模式是一种最好的做法。

1. 从“系统维护”菜单中，单击“备份”。出现“备份 CommandCenter”屏幕。



图 130 备份 CommandCenter 屏幕

2. 在“备份名称”字段内此备份的名称。
3. 在“说明”字段内为此备份键入可选的简短说明。
4. 选择一种“备份类型”。
    - **自定义** – 允许指定将哪些部分添加到备份中，通过在下面的“备份选项”区域内选取。选中下面的每一项将其包含在备份中。
        - o **数据** – CC-SG 配置、设备和节点配置以及用户数据。（标准）
        - o **日志** – CC-SG 上存储的错误日志和事件报告
        - o **CC-SG 固件文件** – 存储用于更新 CC-SG 服务器本身的固件文件。
        - o **设备固件文件** – 存储用于更新受到 CC-SG 管理的 Raritan 设备的固件文件。
        - o **应用程序文件** – 存储供 CC-SG 用于将用户连接到节点的应用程序。
    - **完整** – 为 CC-SG 上存储的所有数据、日志、固件和应用程序文件创建备份。这样产生的备份文件最大。
    - **标准** – 仅创建 CC-SG 上关键数据的备份。此备份包括 CC-SG 配置信息、设备和节点配置以及用户配置。这样产生的备份文件最小。
5. 如果要将此备份文件的副本保存到外部服务器，请选中“备份至远程位置”。
    a. 选择用于连接远程服务器的“协议”：FTP 或 SFTP
    b. 在“主机名”字段中键入服务器的 IP 地址或主机名。
    c. 如果不使用所选协议的默认端口（FTP：21，SFTP：22），请在“端口号”字段中键入所用的通信端口。
    d. 在“用户名”字段内为远程服务器键入用户名。

e. 在“密码”字段内为远程服务器键入密码。

f. 在“目录”字段中，指定在远程服务器上用于存储备份的目录。

6. 单击“确定”。

将出现成功消息确认 CC-SG 备份。备份文件保存在 CC-SG 文件系统内，如果在“备份至远程位置”字段中指定，则也会保存到远程服务器。以后可恢复此备份。

恢复 CC-SG

1. 从“系统维护”菜单中，单击“恢复”。出现“恢复 CommandCenter”屏幕，并显示一个 CC-SG 可用的备份会话表。该表还列出备份类型、备份日期、说明、所备份的 CC-SG 版本以及备份文件的大小。

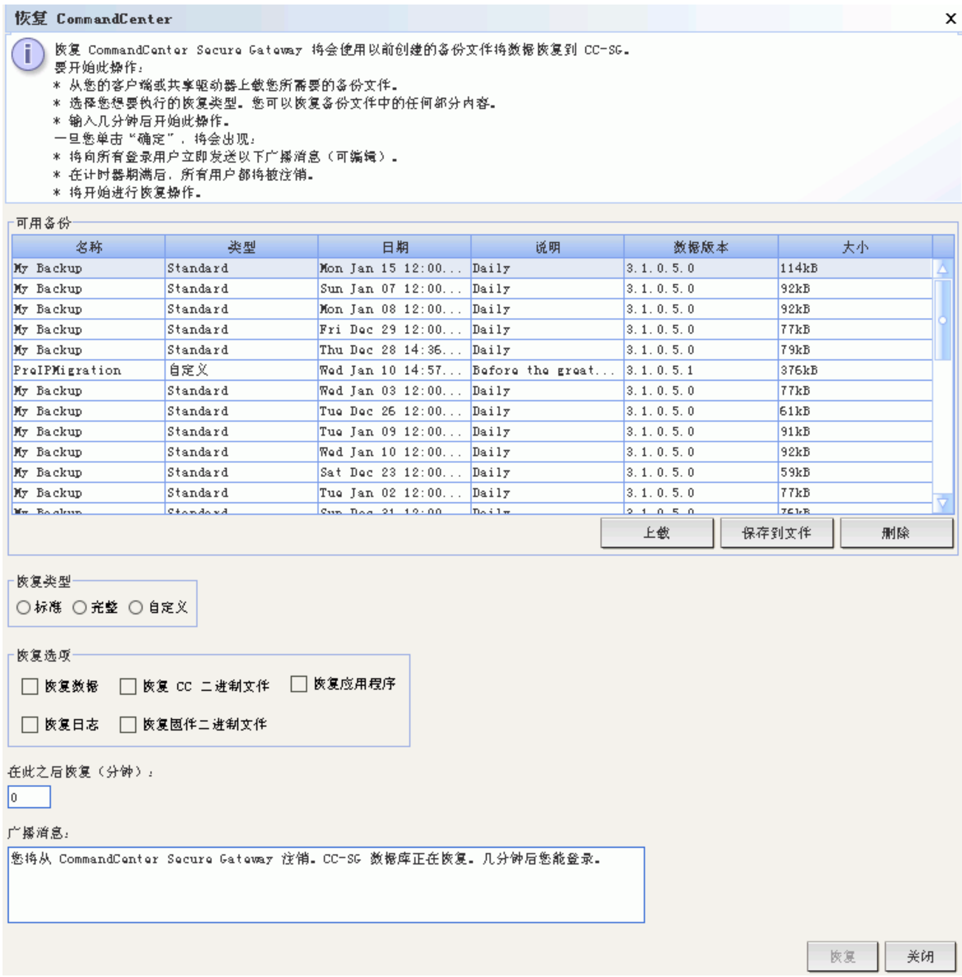


图 131 恢复 CommandCenter 屏幕

2. 如果要从 CC-SG 系统以外存储的备份中恢复，首先要上载使其可用。单击“上载”。出现打开对话屏幕。可从客户端网络的任何位置检索文件。

   a. 浏览备份文件，然后在对话窗口中选择。

   b. 单击“打开”将此文件上载到 CC-SG。

   c. 完成后，备份文件将出现在“可用备份”表内。

3. 从“可用备份”表内选择要恢复的备份。

4. 如果适用，选择从此备份中要执行何种类型的恢复：
   - **标准** – 仅恢复 CC-SG 的关键数据。包括 CC-SG 配置信息、设备和节点配置以及用户配置。
   - **完整** – 恢复备份文件中存储的所有数据、日志、固件和应用程序文件。这需要为文件制作完整备份。
   - **自定义** – 允许指定将备份中的哪些部分恢复到 CC-SG，通过在下面的“恢复选项”区域内选取。选中下面的每一项将其包含在恢复中。
     a. **数据** – CC-SG 配置、设备和节点配置以及用户数据。
     b. **日志** – CC-SG 上存储的错误日志和事件报告
     c. **CC 固件文件** – 存储用于更新 CC-SG 服务器本身的固件文件。
     d. **设备固件文件** – 存储用于更新受到 CC-SG 管理的 Raritan 设备的固件文件。
     e. **应用程序文件** – 存储供 CC-SG 用于将用户连接到节点的应用程序。
5. 在“在此之后恢复”字段中键入 CC-SG 执行恢复操作前将要等待的分钟数，范围是 0-60。这可让用户有时间完成其工作并注销。
6. 在“广播消息”字段中，键入一条消息，通知其他 CC-SG 用户将要进行恢复。
7. 单击“恢复”。

单击“恢复”后，CC-SG 将等待在“在此之后恢复”字段中指定的时间，然后从所选的备份中恢复其配置。恢复开始后，所有其他用户将被注销。

保存和删除备份文件

也可从“恢复 CommandCenter”屏幕上保存和删除 CC-SG 系统上存储的备份。保存备份允许在其它 PC 上维护备份文件的副本，而删除不再需要的备份可节省 CC-SG 上的空间。

要保存备份

1. 从“可用备份”表中，选择要保存到 PC 上的备份。
2. 单击“保存到文件”。出现“保存”对话框。

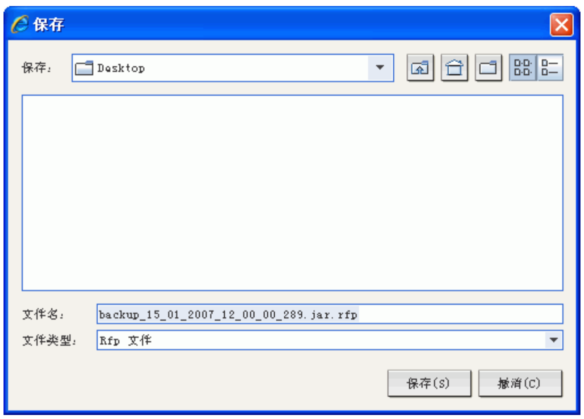


图 132 保存备份文件

3. 指定要保存 CC-SG 备份文件的位置，然后单击“保存”。备份文件将复制到客户端 PC 上。

要删除备份

1. 从“可用备份”表内，选择要删除的备份。
2. 单击“删除”。出现确认对话框。
3. 单击“确定”从 CC-SG 系统中删除备份，或单击“取消”不删除退出。一旦删除，备份文件将从 CC-SG 中删除。

注：保存和恢复可用于在 CC-SG 设备之间移动备份。保存和删除可用于维护 CC-SG 备份的安全存档，无需在系统上存储完整存档。

复位 CC-SG

使用“复位 CommandCenter”命令将清除 CC-SG 数据库的数据。不会复位系统配置数据，例如 CC-SG 的 IP 地址。将执行以下操作：复位 CC-SG 数据库、复位 SNMP 配置、复位到默认固件、将默认固件载入 CC-SG 数据库，并将诊断控制台复位到默认值。

1. 从“系统维护”菜单中，单击“复位”。

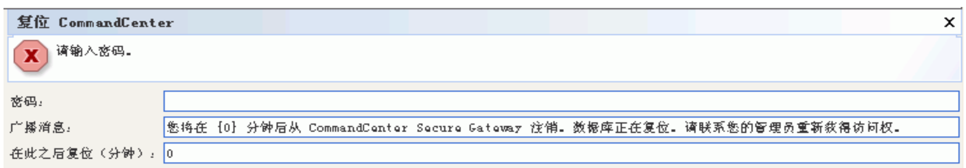


图 133 复位 CC-SG 屏幕

2. 键入 CC-SG 的“密码”。
3. 接受当前的“广播消息”或编辑以创建自己的广播消息。
4. 在“在此之后复位（分钟）”字段中键入 CC-SG 执行复位操作前将要等待的分钟数，范围是 0-60。默认值为 0，即立即复位 CC-SG 设备。
5. 单击“确定”复位 CC-SG 设备。将出现成功消息确认复位。

重要说明：使用“复位”命令将清除 CC-SG 的数据库。所有设备、节点、端口和用户都将被删除。认证也会复位到本地 DB。在使用“复位”之前应备份 CC-SG。

重新启动 CC-SG

重新启动命令用于重新启动 CC-SG 软件。重新启动 CC-SG 将把所有活动用户从 CC-SG 中注销。

注：重新启动不会循环 CC-SG 的电源。要执行完整的重启操作，需要访问诊断控制台，或者在设备上打开电源开关。

1. 从“系统维护”菜单中，单击“重新启动”。出现“重新启动 CommandCenter”屏幕。

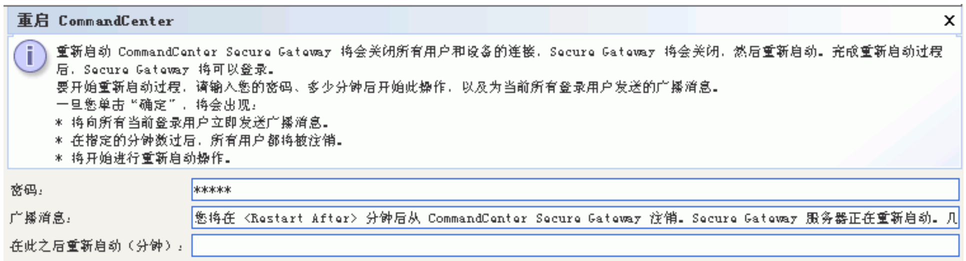


图 134 重新启动屏幕

2. 在“密码”字段内键入密码。
3. 接受默认消息，或在“广播消息”字段中键入向所有当前在线用户显示的警告消息（例如，可能需要给用户一点时间完成他们在 CC-SG 中的任务，或告诉他们为何要重新启动系统）。重新启动 CC-SG 后，所有用户将被断开连接。
4. 在“在此之后重新启动（分钟）”字段中键入 CC-SG 执行重启操作前将要等待的分钟数，范围是 0-60。
5. 单击“确定”重启 CC-SG，或单击“取消”不重启退出屏幕。一旦重新启动 CC-SG，即会显示广播消息。
6. 单击“确定”重新启动 CC-SG。CC-SG 将重新启动，准备就绪使用。

升级 CC-SG

升级命令用于将 CC-SG 固件升级到更新的版本。要升级 CC-SG，应先在客户端 PC 上存有最新的固件文件。可从 Raritan 网站上的“支持”部分下载固件文件：
http://www.raritan.com/support/sup_upgrades.aspx
建议在升级前首先备份 CC-SG。

注：如果在操作 CC-SG 群集，则必须首先删除群集，然后单独升级每个节点。

1. 在“系统维护”菜单中，单击“维护模式”，然后单击“进入维护模式”将 CC-SG 置于维护模式。不执行这一操作将不能升级 CC-NOC。详情参阅本章的“维护模式”部分。
2. CC-SG 处于维护模式后，在“系统维护”菜单中单击“升级”。出现“升级 CommandCenter”屏幕。

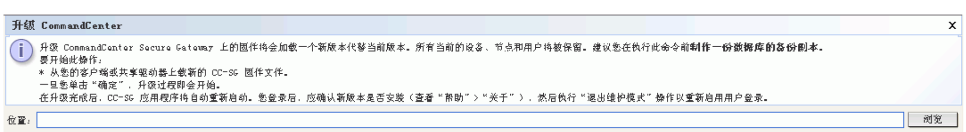


图 135 升级 CC-SG 屏幕

3. 单击“浏览”，导航并选择 CC-SG 固件文件，然后单击“打开”。
4. 单击“确定”将固件文件上载到 CC-SG。
5. 固件文件上载到 CC-SG 以后，将收到一条成功消息。这表示 CC-SG 已经收到文件，并已经开始升级过程。此时所有用户将从 CC-SG 断开连接。单击“确定”退出 CC-SG 并允许其重新启动。
6. 必须等待大约 8 分钟让 CC-SG 重新启动。关闭浏览器窗口，然后清除浏览器高速缓存。
7. 8 分钟后，打开新的浏览器窗口并启动 CC-SG。在“帮助”菜单中，单击“关于 Raritan Secure Gateway”。在出现的窗口中，检查版本号以验证升级是否成功。如果版本未升级，请重复上面的步骤。如果升级成功，请继续进行下一步。
8. CC-SG 将仍处于维护模式，这意味着大部分用户不能登录。要退出维护模式，在“系统维护”菜单中单击“维护模式”，然后单击“退出维护模式”。单击“确定”。

关闭 CC-SG

以下是为管理员关闭 CC-SG 的建议方法。关闭 CC-SG 将关闭 CC-SG 软件，但不会关闭 CC-SG 设备的电源。

1. 从“系统维护”菜单中，单击“关闭 CommandCenter”。出现“关闭 CommandCenter”屏幕。

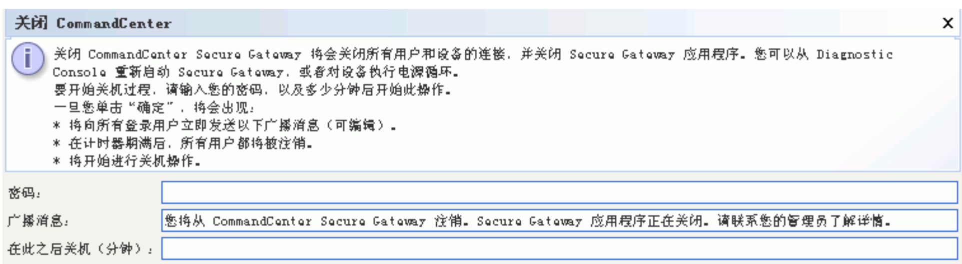


图 136 关闭 CC-SG 屏幕

2. 在“密码”字段内键入密码。
3. 接受默认消息，或在“广播消息”字段中键入向所有当前在线用户显示的消息（例如，可能需要给用户一点时间完成他们在 CC-SG 中的任务，并告诉他们何时可以重新正常使用系统）。关闭 CC-SG 后，所有用户将被断开连接。
4. 在“在此之后关机（分钟）”字段中键入 CC-SG 执行关机操作前将要等待的分钟数，范围是 0-60。
5. 单击“确定”关闭 CC-SG，或单击“取消”不关闭退出屏幕。一旦关机，即出现 CC-SG 登录窗口。

注：CC-SG 关机后，所有用户将被注销并重新定向到登录屏幕。在按下节所述重新启动 CC-SG 之前，用户不能重新登录。

关机后重启 CC-SG

关闭 CC-SG 后，使用下面两种方法之一重新启动设备：

1. 使用诊断控制台。详情参见**第 12 章：高级管理**中的“诊断控制台”。
2. 循环 CC-SG 设备的电源。

结束 CC-SG 会话

注销

要在会话结束后退出 CC-SG，或在登录时自己或其它用户进行更改后要刷新数据库，需要从 CC-SG 中完全注销，然后重新登录。

1. 在“Secure Gateway”菜单上，单击“注销”。出现“注销”窗口。
2. 单击“是”从 CC-SG 中注销，或单击“否”关闭窗口。一旦注销，即出现 CC-SG 登录窗口。
3. 重新登录 CC-SG，或单击“退出”完全关闭 CC-SG。

退出 CC-SG

任何时候想要退出 CC-SG，即可退出。

1. 在“Secure Gateway”菜单上，单击“退出”。出现“退出”窗口。
2. 单击“是”退出 CC-SG，或单击“否”关闭“退出”窗口继续工作。

第 12 章：高级管理

指导设置

“指导设置”指导管理员分步完成 CC-SG 上一些最常见的任务：创建关联、设置 Raritan 设备、创建用户组和创建用户。有关运行“指导设置”的信息，请参阅**第 3 章：使用指导设置配置 CC-SG**。

当日消息设置

“当日消息”功能允许 Secure Gateway 管理员提供一条所有用户在登录时可以看到的消息。要配置当日消息，管理员必须有“CC 设置和控制”权限。

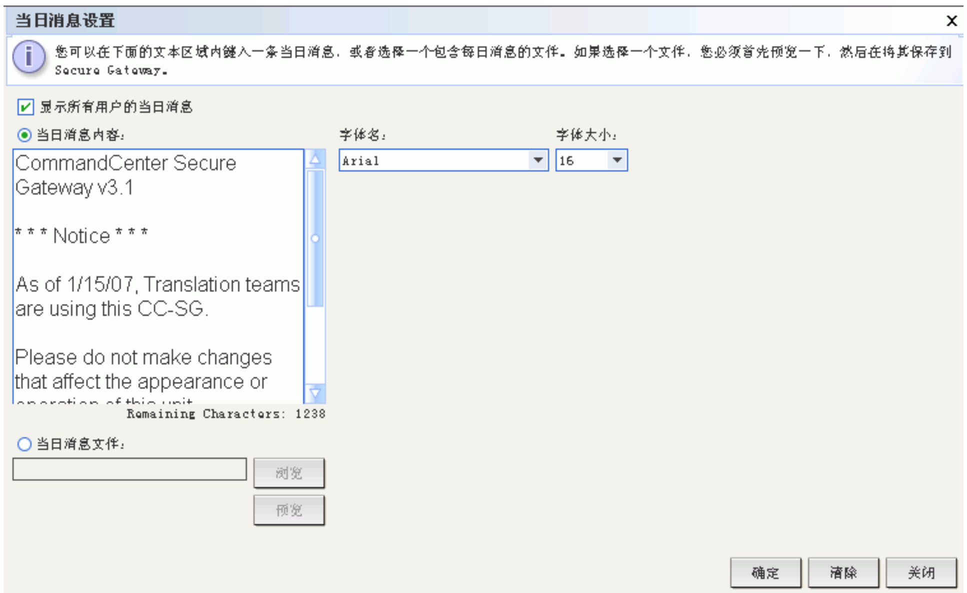


图 137 配置当日消息

1. 在“管理”菜单中单击“当日消息设置”。出现当日消息设置屏幕。
2. 如果要在所有用户登录时为其显示消息，请选中“显示所有用户的当日消息”。
3. 如果要在 CC-SG 中键入一条消息，则选择“当日消息内容”；如果要从现有文件中载入消息，则选择“当日消息文件”。

   如果选择“当日消息内容”：

   a. 在提供的对话框中键入消息。
   b. 单击“字体名称”下拉菜单，选择显示消息的字体。
   c. 单击“字体大小”下拉菜单，选择显示消息的字体大小。

   如果选择“当日消息文件”：

   a. 单击“浏览”浏览消息文件。
   b. 在打开的对话窗口中选择文件，然后单击“打开”。
   c. 单击“预览”复查文件的内容。
4. 如果要删除“当日消息内容”对话框中的内容，或者删除“当日消息文件”的路径，请单击“清除”。
5. 单击“确定”将设置保存到 CC-SG。

应用程序管理器

“应用程序管理器”为管理员提供一个界面向 CC-SG 添加访问应用程序，编辑现有应用程序，以及设置访问 Raritan 设备上节点的默认应用程序。

从“管理”菜单中，单击“应用程序”。出现“应用程序管理器”屏幕。

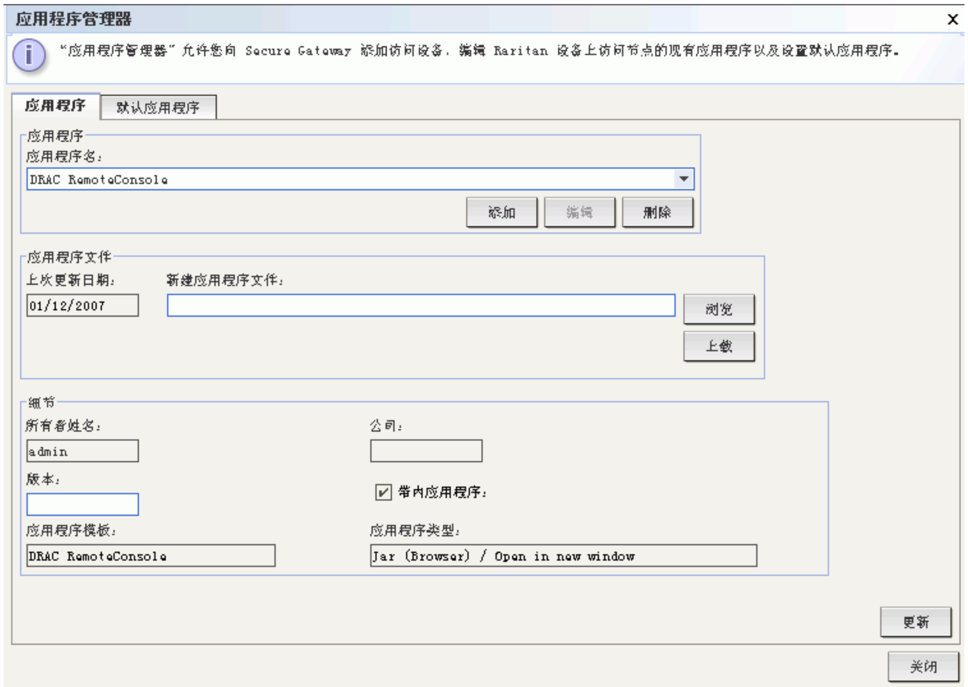


图 138 应用程序管理器的应用程序选项卡

添加、编辑和删除应用程序

单击“应用程序管理器”的“应用程序”选项卡可添加、编辑或删除应用程序。

添加应用程序

1. 在“应用程序”选项卡的“应用程序”部分，单击“添加”。出现“添加应用程序”对话窗口。



图 139 添加应用程序

2. 在“应用程序名称”字段内键入应用程序的名称。

3. 从“可用”列表中选择应用程序将要使用的 Raritan 设备，然后单击“添加”将其添加到“已选定”列表。添加应用程序后，“已选定”列表中的设备将能够选择此应用程序用于访问。如果设备同时提供 KVM 和串行访问，则为每种方法将设备列出两次。
4. 要删除使用应用程序的设备，从“已选定”列表中选择设备，然后单击“删除”。选择所需的设备使用应用程序以后，单击“确定”。出现“打开”对话窗口。
6. 在“打开”对话窗口中，浏览应用程序文件（通常为 .jar 或 .cab 文件）的位置，选择该文件，然后单击“打开”。

然后，所选的应用程序将被载入 CC-NOC。

编辑应用程序

1. 在“应用程序”选项卡的“应用程序”部分中，从“应用程序名称”下拉菜单选择一个应用程序。所选应用程序的详细信息将出现在选项卡的“详细信息”区域内。
2. 取决于应用程序，有些详细信息是可以配置的。根据需要，在“详细信息”区域内配置参数。
3. 单击“编辑”。出现“编辑应用程序”窗口。
4. 如果需要，从“可用”列表中选择应用程序将要使用的其它 Raritan 设备，然后单击“添加”将其添加到“已选定”列表。
5. 如果需要删除使用应用程序的设备，从“已选定”列表中选择设备，然后单击“删除”。
6. 选择所需的设备使用应用程序以后，单击“确定”。

删除应用程序

1. 在“应用程序”选项卡的“应用程序”部分中，从“应用程序名称”下拉菜单选择一个应用程序。所选应用程序的详细信息将出现在选项卡的“详细信息”区域内。
2. 单击“删除”删除所选的应用程序。出现一个确认对话框。
3. 单击“是”确认，或单击“否”取消而不删除应用程序。

默认应用程序

单击“默认应用程序”选项卡可查看和编辑各种接口和端口类型的当前默认应用程序。当配置节点允许通过所选接口进行访问时，在此列出的应用程序将成为默认。



图 140 默认应用程序列表

要编辑某个接口或端口类型的默认应用程序：

1. 选择接口或端口类型所在的行。
2. 双击该行上列出的应用程序。该值变成一个下拉菜单。注意变灰的值不能编辑。
3. 在下拉菜单中，选择连接到突出显示的接口或端口类型时要使用的默认应用程序。如果选择“自动检测”，则 CC-SG 基于客户端浏览器自动检测应用程序。所有默认应用程序均已配置后，单击“更新”保存对 CC-SG 所做的选择。

任何时候单击“关闭”，即可关闭“应用程序管理器”屏幕。

固件管理器

CC-SG 存储 Raritan 设备的固件，使设备更新处于自己的控制之下。固件管理器用于从 CC-SG 中上载设备固件文件或从中删除。

上载固件

此命令允许将不同的固件版本上载到系统。当新的固件版本可用时，将会在 Raritan 网站上发布。

1. 从“管理”菜单中，单击“固件”。出现“固件管理器”屏幕。

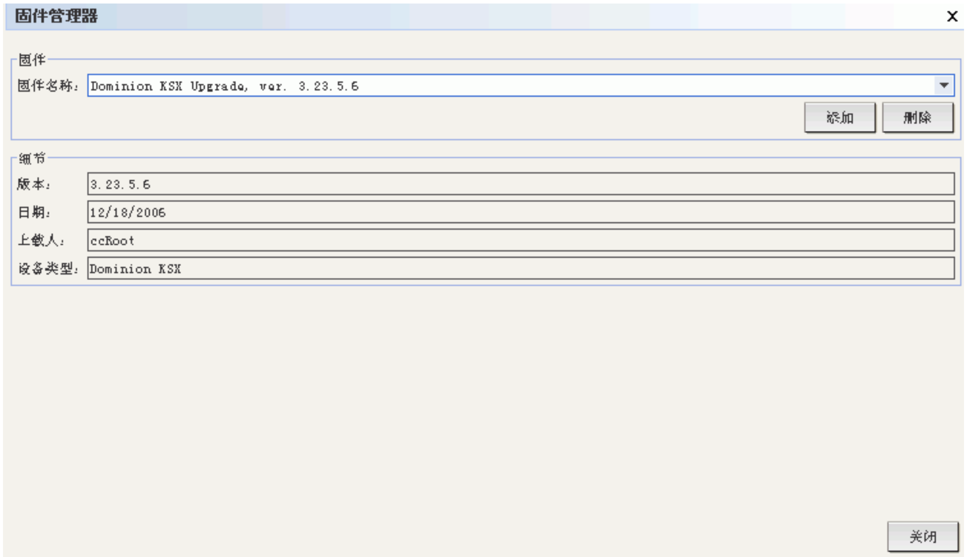


图 141 固件管理器屏幕

2. 单击“添加”添加新固件文件。出现搜索窗口。

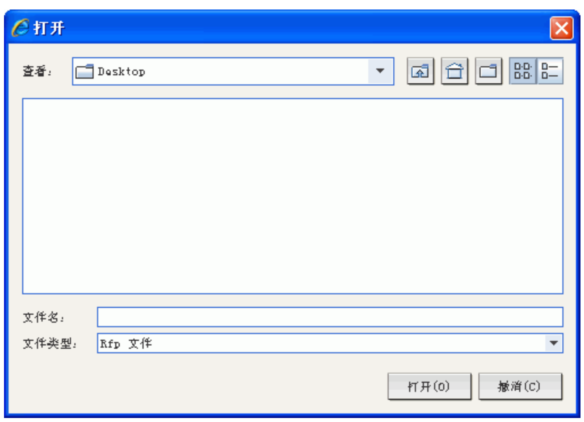


图 142 固件搜索窗口

3. 单击“查找位置”下拉箭头，在系统中导航并找到固件文件。找到固件后，选择并单击“打开”。添加后，在“固件管理器”的“固件名称”字段内出现固件的名称。

删除固件

1. 从“管理”菜单中，单击“固件”。出现“固件管理器”屏幕。
2. 单击“固件名称”下拉箭头并选择要删除的固件。
3. 单击“删除”。出现“删除固件”窗口。



图 143 删除固件窗口

4. 单击“是”删除固件，或单击“否”关闭窗口。
5. 单击“关闭”关闭“固件管理器”屏幕。

配置管理器

“配置管理器”是管理几种 CC-SG 核心设置的地方，例如网络配置。

网络配置

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
2. 单击“网络设置”选项卡。

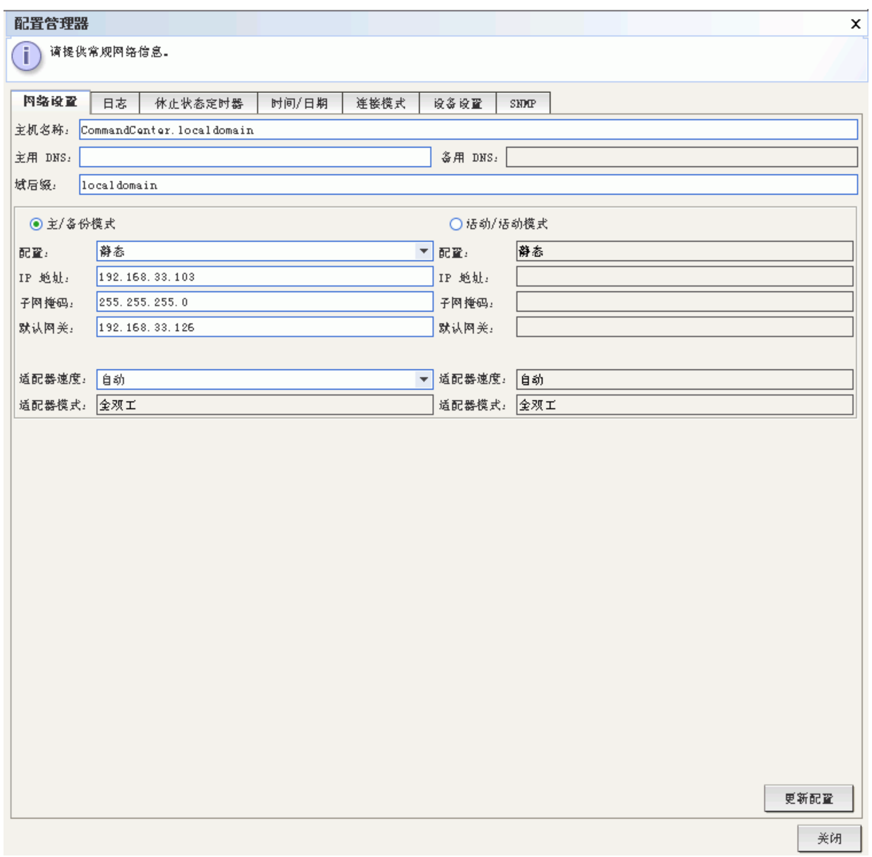


图 144 配置管理器网络设置屏幕

3. 在“主机名称”字段内键入 CC-SG 主机名。有关主机名规则，请参阅本指南的第 1 章。一旦选中“更新配置”，如果已经配置域服务器和域后缀，则将会刷新字段以反映完全限定的域名 (FQDN)。
4. 单击“主/备份模式”或“活动/活动模式”。一个 CC-SG 提供两个网络接口控制器 (NIC)。在 G1 或 V1 设备上的 NIC 从左向右标记，位于设备的后部，详见下表：

型号	最左侧 NIC（主用接口）	最右侧 NIC
G1	LAN1	LAN0
V1	LAN1	LAN2

E1 设备上的 NIC 则不同，详见下表：

型号	顶部 NIC（主用接口）	底部 NIC
E1	LAN1	LAN2

一个接口可自己使用，或者可两个同时使用。为了简单起见，下面的讨论使用 LAN1 作为左侧 NIC（主用），LAN2 作为右侧 NIC。有些内部诊断和消息可能将这些接口称为“eth0”和“eth1”。

注：如果两个接口都断开连接，则 CC-SG 将重新启动。

5. 选择“主/备用模式”以实现网络故障切换和冗余。在这种模式下，在某个时间点只有一个 NIC 活动，只能分配一个网络 IP 地址。

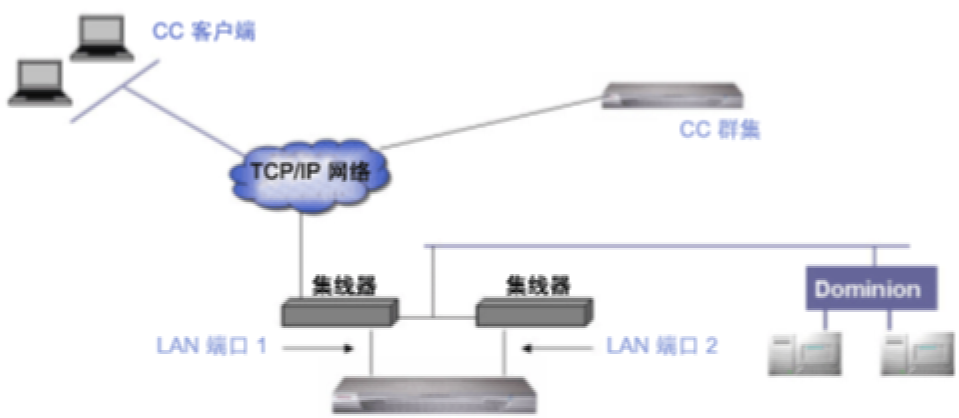


图 145 主用/备用网络

通常两个 NIC 都连接到同一个 LAN 子网，但可使用不同的交换机（或集线器）来提高可靠性。使用两个 NIC 时，提供网络级别的冗余。例如，如果 LAN1 已连接并收到“链路完整”信号，则 CC-SG 使用此 NIC 进行所有的通信。如果 LAN1 失效而 LAN2 已连接，CC-SG 将把分配（可能由 DHCP 分配）IP 地址移植到 LAN2。将会使用 LAN2 直到 LAN1 修复并返回服务。这时，CC-SG 恢复使用 LAN1。

只要一个接口可用，PC 客户端就不会在失效时注意到服务中断。CC-SG 保持同一个逻辑 IP 地址，但在可能出现网络失效时将尝试保持通信通道和现有会话的运行。所有通信（例如 PC 客户端、Raritan 设备管理、群集对端等）都承载在这个由两个 NIC 维护的单个通信通道上。

6. 如果网络条件特殊，尤其是有两个可能不存在路由的网络时，选择“活动/活动模式”。如果网络安全非常重要，并且使用代理类型的部署，则也应选择这种模式。

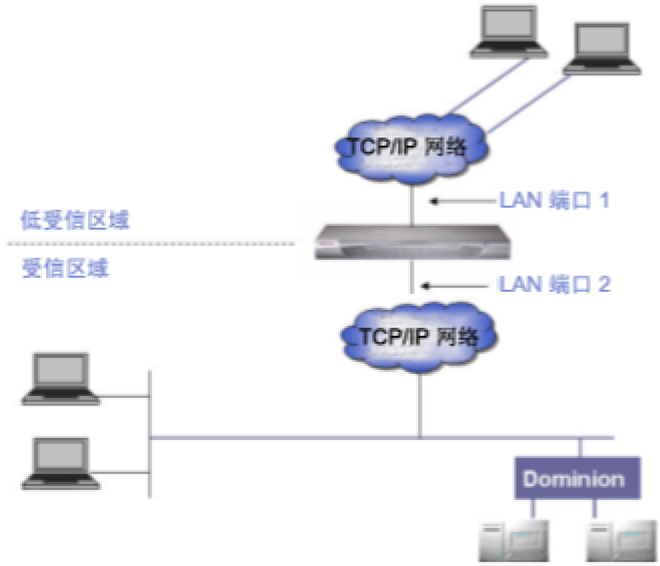


图 146 活动/活动网络

在这种模式下，CC-SG 充当一个两个单独 IP 域之间的“路由器”或“交通警察”，特别是使用“代理”模式时。（详情参阅本章后面的“连接模式”部分）。在代理模式下，需要“活动/活动”模式，使 CC-SG 能将代理的 PC 客户端会话路由到各自的节点。建议将 Raritan 控制的设备连接到 LAN1，而代理的 PC 客户端连接到 LAN2。两个 NIC 应在单独的子网上——但如果使用 DHCP，这可能无法实现，因此这种配置将无法支持。在配置两个 NIC 时，仅对一个 NIC 指定默认的网关地址，将另一个留空。当一个 NIC 失效时，CC-SG 尝试根据当前的 IP 路由表从其它 NIC 路由数据包。这种路由可能不成功，尤其是使用防火墙时。如果需要其它路由，则可在诊断控制台上添加。详情参阅本章后面的“编辑静态路由（网络接口）”部分。

***注：**使用“活动/活动”模式时无法配置群集。*

7. 单击“配置”下拉箭头并从列表中选择“DHCP”或“静态”。如果选择 DHCP 且 DHCP 服务器已正确配置，则键入主机名。选择“更新配置”后，将自动填充 DNS 信息、域前缀、IP 地址、默认网关和子网掩码。CC-SG 使用这些信息动态地向 DNS 服务器注册（如果接受动态更新）。成功注册后，即可通过主机名访问 CC-SG，因为使用 DHCP 时可能不知道 IP 地址。

   如果选择“静态”，请在相应的字段中键入“IP 地址”、“子网掩码”、“默认网关”、“主用 DNS”和“备用 DNS”信息。同时，在“域后缀”中为域设置键入一个字符串。
8. 单击“适配器速度”下拉箭头并从列表中选择一个线速。
9. 如果在“适配器速度”字段中选择“自动”，则“适配器模式”字段将被禁用，“全双工”自动选择。如果在“适配器速度”内不是指定“自动”，则单击“适配器模式”下拉箭头并从列表中选择一个双工模式。
10. 如果选择“活动/活动”模式，请按照第 5 到 7 步配置第二个网络接口。
11. 单击“更新配置”即更新系统的网络设置。
12. 单击“关闭”关闭“配置管理器”屏幕。

日志配置

从“日志”选项卡上，可配置 CC-SG 向外部日志服务器发送报告。可配置每个日志中报告的消息级别。

配置日志活动

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
2. 单击“日志”选项卡。

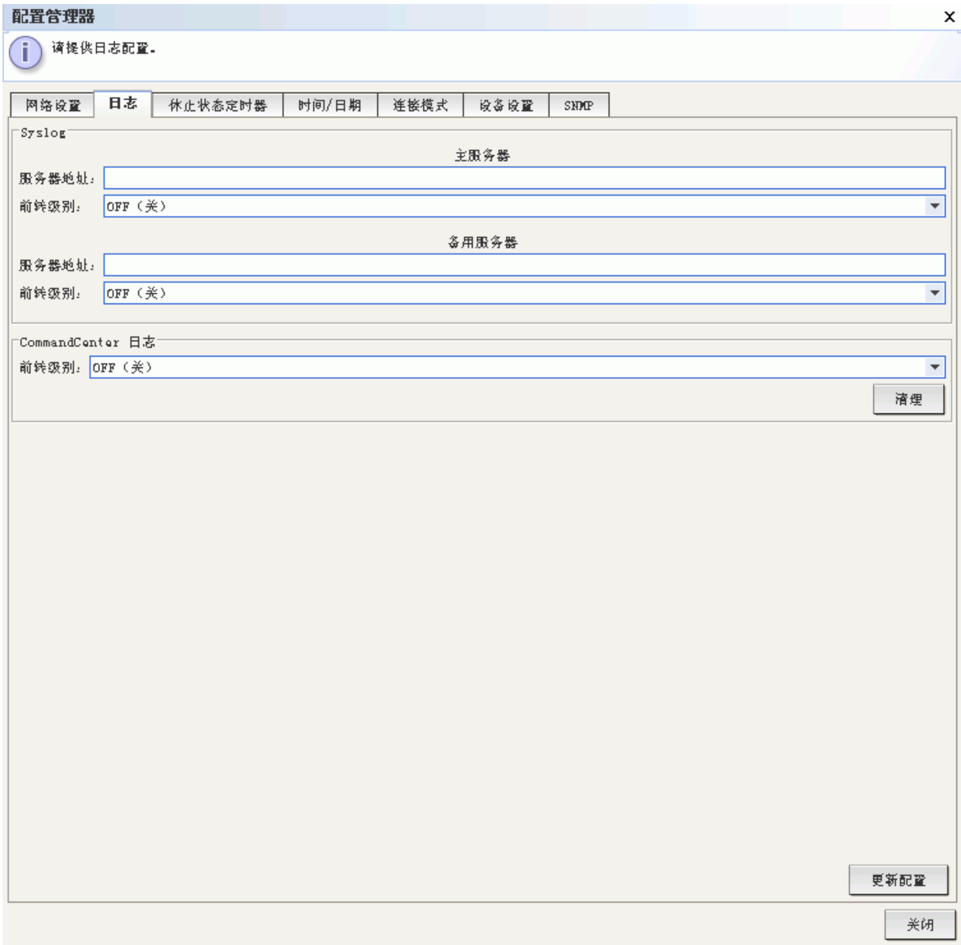


图 147 配置管理器日志屏幕

3. 要指定 CC-SG 使用的外部日志服务器，请在“主用服务器”下面“服务器地址”中键入 IP 地址。
4. 单击“前转级别”下拉箭头并选择一个事件严重程度级别。在此级别及以上级别的所有事件将被发送到日志服务器。
5. 要配置第二台日志服务器，请重复第 3 和 4 步填写“备用服务器”下面的字段。
6. 在“CommandCenter 日志”下面，单击“前转级别”下拉菜单并选择一个严重程度级别。在此级别及以上级别的所有事件将在 CC-SG 自己的内部日志中报告。
7. 配置日志完成以后，单击“更新配置”保存对 CC-SG 所做的设置。
8. 单击“关闭”关闭“配置管理器”屏幕。

清除 CC-SG 内部日志

“日志”选项卡还可以用于清除 CC-SG 的事件日志。此命令仅清除 CC-SG 的事件日志，而不会清除外部日志服务器所记录的事件。

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
2. 单击“日志”选项卡。
3. 单击屏幕底部的“清除”。出现一个确认对话窗口。
4. 单击“是”即清除 CC-SG 的事件日志。

***注：**“审计跟踪”和“错误日志”报告基于 CC-SG 的内部日志。如果清除 CC-SG 的内部日志，这两个报告也将清除其数据。*

休止状态定时器配置

使用此屏幕配置一个会话可保持活动多长时间，此时间过后将被注销。

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
3. 单击“休止状态定时器”选项卡。



图 148 休止状态定时器选项卡

3. 在“休止时间”字段中键入希望的休止时间限制（单位是秒）。
4. 单击“更新配置”将设置保存到 CC-SG。

时间/日期配置

CC-SG 的时间和日期必须准确维护，从而提供其设备管理功能的可信性。

重要事项！在“任务管理器”中计划任务时将用到此时间/日期配置。详情参见第 12 章：高级管理中的“任务管理器”。在客户端上设置的时间可能不同于 CC-SG 上设置的时间。

只有 CC 超级用户以及拥有类似权限的用户可以配置时间和日期。

1. 从“管理”菜单中，单击“配置”打开“配置管理器”屏幕。
2. 单击“时间/日期”选项卡。

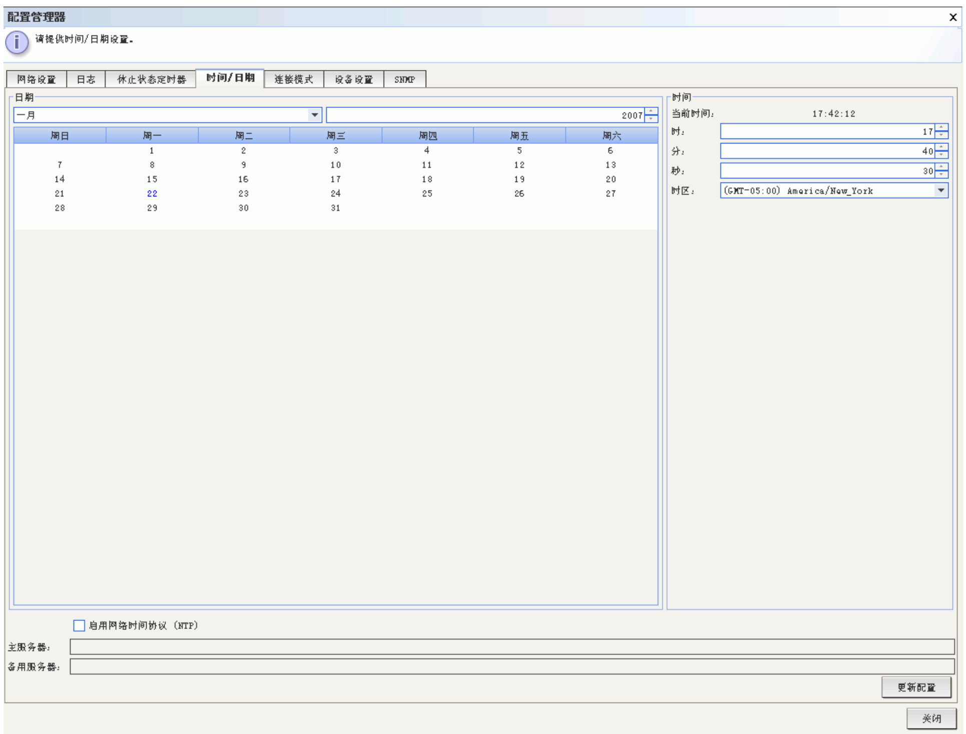


图 149 配置管理器时间/日期屏幕

a. **手动设置日期和时间：日期**——单击下拉箭头选择“月”，使用上/下箭头选择“年”，然后在日历区域选择“天”。**时间**——使用上/下箭头设定“时”、“分”和“秒”，然后单击“时区”下拉箭头选择操作 CC-SG 所在的时区。

b. **要通过 NTP 设置日期和时间：**选中窗口底部的“启用网络时间协议”复选框，在相应的字段中键入“主用 NTP 服务器”和“备用 NTP 服务器”的 IP 地址。

注：网络时间协议 (NTP) 是将所连计算机的日期和时间数据与基准 NTP 服务器进行同步的协议。CC-SG 配置 NTP 后，即可与公共可用的 NTP 基准服务器同步时钟时间，并维护正确和一致的时间。

3. 单击“更新配置”将时间和日期更改应用到 CC-SG。
4. 单击“刷新”即在“当前时间”字段中重新载入新的服务器时间。
5. 从“维护”菜单中，单击“重新启动”即重启 CC-SG。

注：在群集配置上禁用更改时区。

调制解调器配置

此屏幕用于从客户端机器通过拨号连接访问 CC-SG G1。这种访问 CC-SG 的方法可在紧急情况下使用。

注：在 V1 或 E1 平台上不提供调制解调器，故无法配置。

配置 CC-SG

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕时，单击“调制解调器”选项卡。

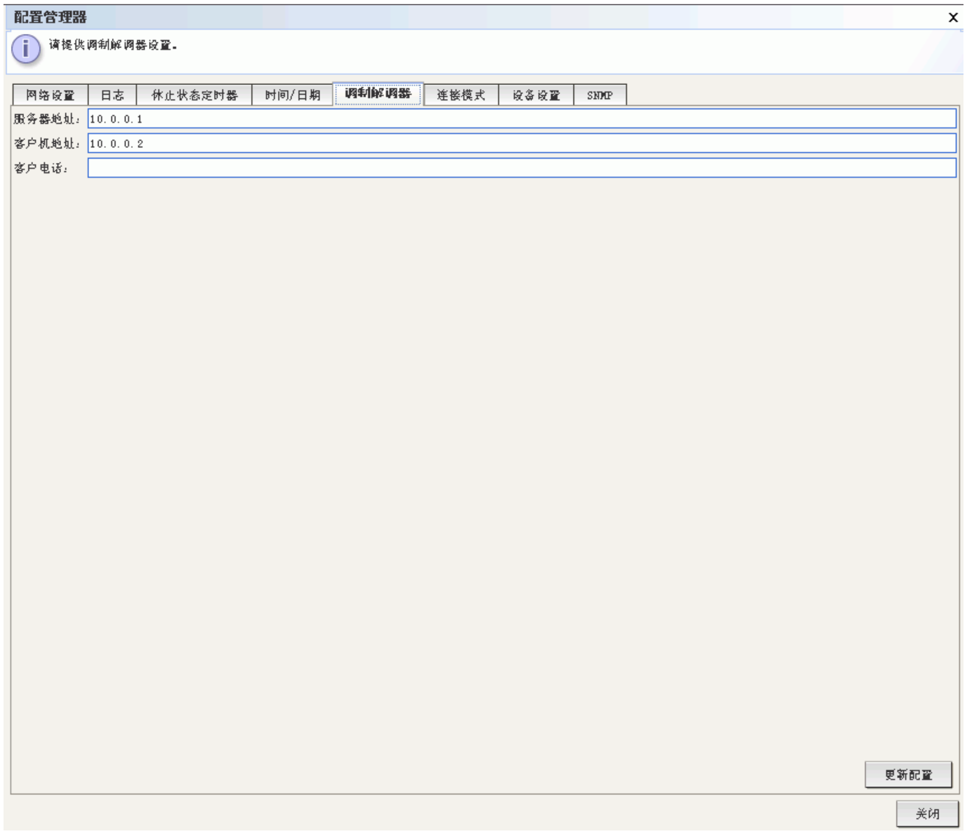


图 150 配置管理器调制解调器屏幕

2. 在“服务器地址”字段中键入 CC-SG 的 IP 地址。
3. 在“客户端地址”字段中键入将要拨入 CC-SG 的客户端的 IP 地址。
4. 如果使用回拨呼叫，在“客户端电话”字段中键入 CC-SG 拨号连接客户端的回拨号码。
5. 单击“更新配置”保存调制解调器信息。

在客户端 PC 上配置调制解调器

将电话线连接到带有内置调制解调器的 CC-SG G1。可以去掉 LAN 电缆。

在将要拨号的客户端上，将调制解调器连接到客户端机器（如 Windows XP 机器）。将电话线连接到客户端调制解调器。重启客户端机器，则所连的调制解调器被发现为新设备。按照以下步骤在客户机（假设为 Windows XP 客户端机器）上安装调制解调器：

1. 选择“控制面板”→“电话和调制解调器选项”。
2. 单击“调制解调器”选项卡。



图 151 调制解调器选项卡

3. 单击“属性”。
4. 单击“高级”选项卡。

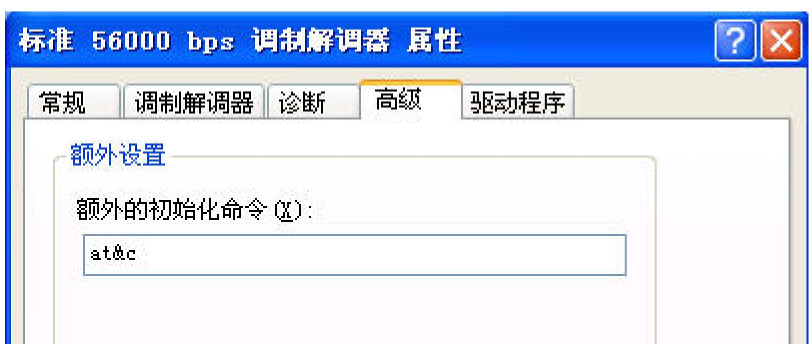


图 152 额外的初始化命令

5. 在“额外的初始化命令”中键入一个初始化命令，调制解调器将用来设置“载波检测”标记。例如，对于 SoftK56 Data Fax 调制解调器键入“**at&c**”。这将告诉 Windows 在另一侧（拨入侧）关闭调制解调器连接时，不要关闭启动的调制解调器连接。单击“确定”保存设置。

配置拨号连接

下面的过程介绍如何从 Windows XP 客户端机器上创建一个到 CC-SG 的入站拨号连接。

1. 在“开始”菜单上，单击“我的网络位置”。
2. 在窗口中右键单击，选择“属性”。
3. 在“网络连接”窗口中的“网络任务”下，单击“创建一个新的连接”。



图 153 创建新连接

4. 单击“下一步”，“连接到我的工作场所的网络”，“拨号连接”。
5. 键入 CC-SG 的名称，例如 CommandCenter。

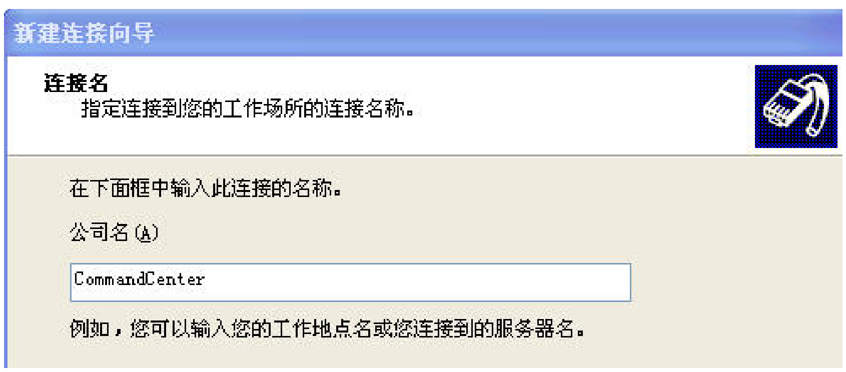


图 154 连接名称

6. 键入用于连接 CC-SG 的电话号码，然后单击“下一步”。这不是在 CC-SG 上的“配置管理器”内“调制解调器”选项卡下面配置为“客户端电话”的回叫号码。

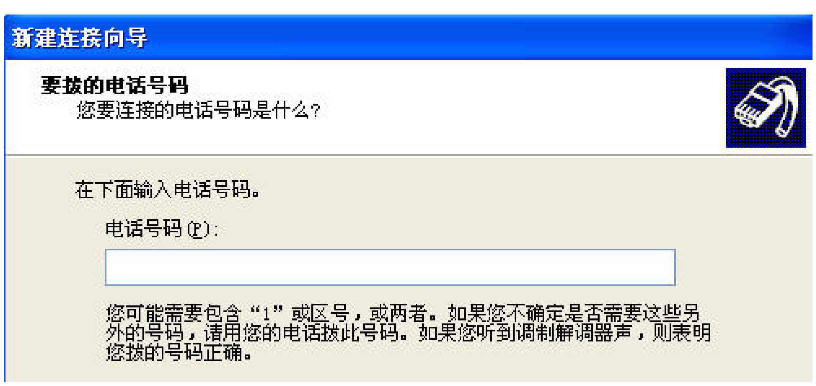


图 155 要拨打的电话号码

7. 拨入 CC-SG 不需要智能卡。如果不使用智能卡，为此连接单击“不使用我的智能卡”，然后单击“下一步”。
8. 在下一个屏幕上，通常要单击“仅我自己使用”使其仅为自己所用。
9. 在最后一个屏幕上单击“完成”保存连接设置。

配置回拨连接

如果 CC-SG 使用回拨连接，需要使用下面介绍的脚本文件。要提供脚本文件用于回拨：

1. 在“开始”菜单上，单击“我的网络位置”。
2. 单击“网络任务”下面的“查看网络连接”。
3. 右键单击 CommandCenter 连接，然后单击“属性”。
4. 单击“安全性”选项卡。

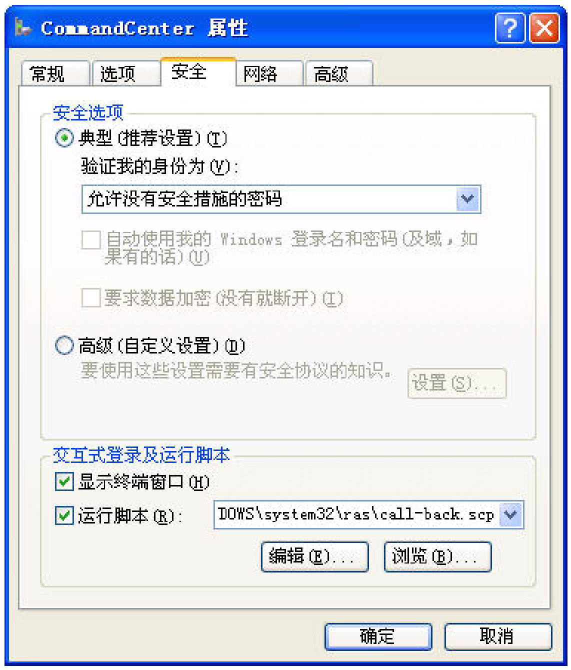


图 156 指定拨号脚本

5. 单击“显示终端窗口”。
6. 单击“运行脚本”并单击“浏览”以输入拨号脚本，例如 call-back.scp。
7. 单击“确定”。

<u>回拨脚本文件示例：</u>

```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
```

waitfor "ogin:"
transmit "ccclient^M"
endproc

使用调制解调器连接 CC-SG

要连接 CC-SG：

1. 在“开始”菜单上，单击“我的网络位置”。
2. 单击“网络任务”下面的“查看网络连接”。
3. 双击 CommandCenter 连接。



图 157 连接 CC-SG

4. 键入用户名“ccclient”，密码“cbupass”。



图 158 输入用户名和密码

5. 如果尚未填写用于连接 CC-SG 的电话号码，请在此输入电话号码。这不是回拨号码。
6. 单击“拨号”。如果使用回拨，调制解调器将拨叫 CC-SG，然后 CC-SG 将拨叫客户端 PC。

7. 如果在本章上文的“**配置回拨连接**”一节选中“显示终端窗口”，则会出现类似下面的窗口：

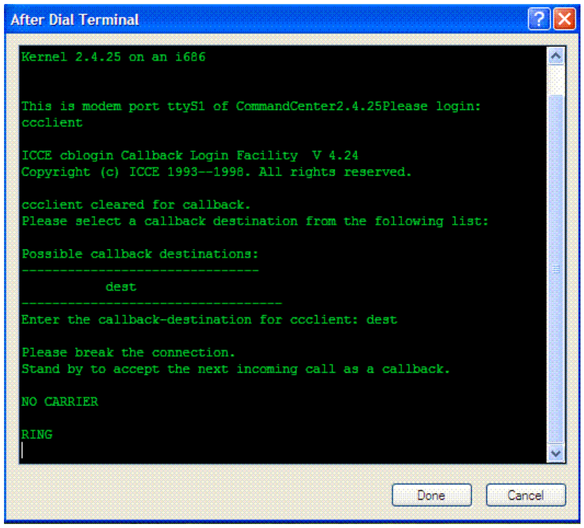


图 159 拨叫后终端

8. 等待 1 到 2 分钟，在支持的浏览器内输入 CC-SG 的 IP 地址（在 CC-SG 上“配置管理器”中“调制解调器”选项卡下“服务器地址”内配置的 IP 地址），登录 CC-SG。

连接模式

连接到节点后，即可选择与该节点直接来回传递数据（直接模式），或通过 CC-SG 设备路由所有数据（代理模式）。虽然“代理模式”增加 CC-SG 服务器上的带宽负荷，但仅需要在防火墙上保持打开 CC-SG TCP 端口（80、443 和 2400）。请参阅 Raritan 的《数字解决方案部署指南》了解详情。

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
2. 单击“连接模式”选项卡。

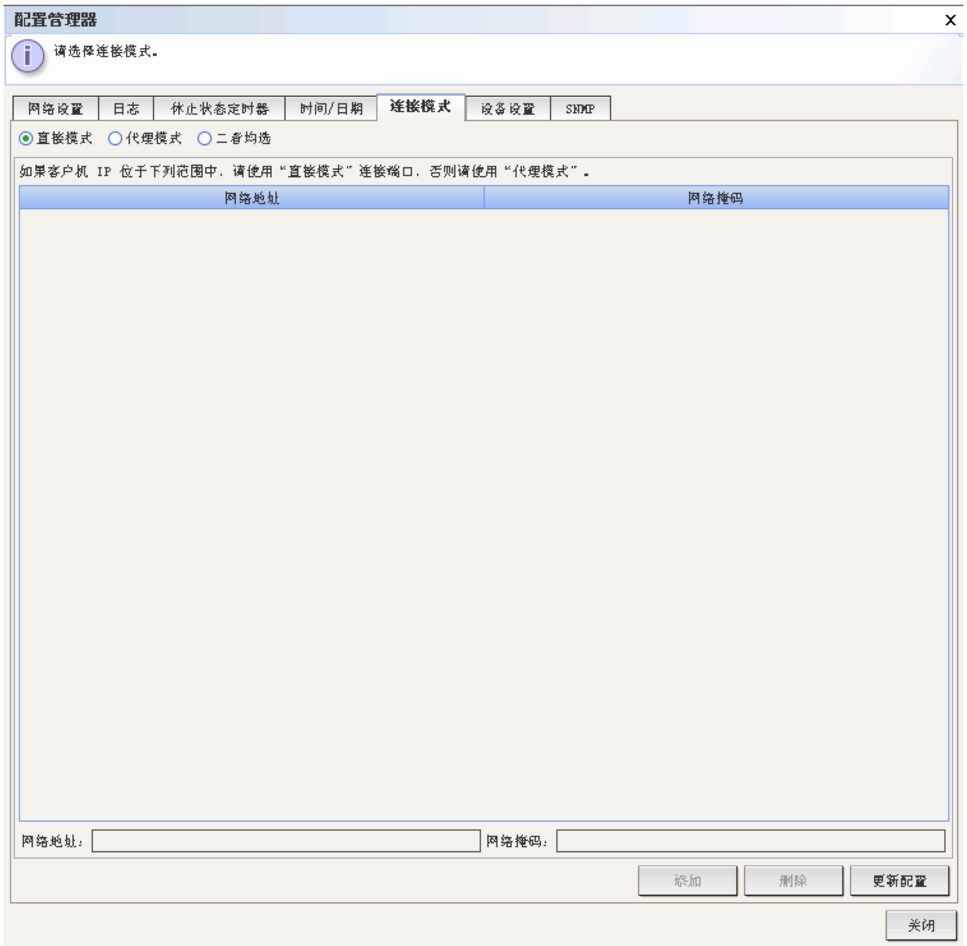


图 160 配置管理器连接屏幕——直接模式

3. 单击所需的连接模式单选按钮。
   a. 单击“直接模式”单选按钮直接连接设备。
   b. 单击“代理模式”单选按钮通过 CC-SG 设备连接设备。
   c. 如果想要直接连接部分设备，但又通过“代理模式”连接其它设备，则单击“二者均选”单选按钮。然后指定需要直接连接的设备的设置。
      i. 在屏幕底部的“网络地址”字段内键入客户端 IP 地址。
      ii. 在“网络掩码”字段内键入客户端网络掩码。
      iii. 单击“添加”按钮将“网络地址”和“网络掩码”添加到屏幕上。（可能需要使用屏幕右侧的滚动条才能看到“添加”/“删除”/“更新配置”按钮）

设备设置

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
2. 单击“设备设置”选项卡。

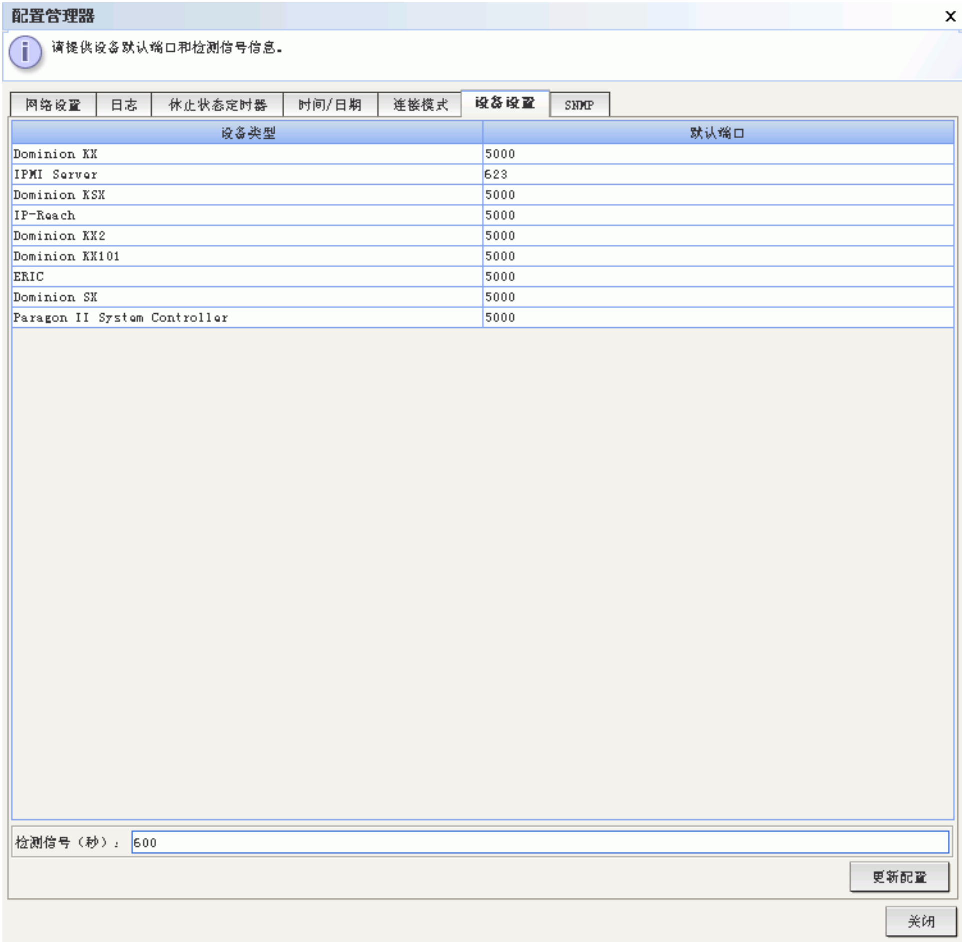


图 161 配置设置设备设置屏幕

3. 要更新设备的默认端口，在表中选择一个“设备类型”，然后双击“默认端口”的值。键入新的默认端口值，然后按回车键。
4. 要更新设备超时时长，双击屏幕底部的“检测信号（秒）”值。键入此设备的新的超时时长。
5. 单击“更新配置”保存新的设备值。将出现成功消息确认所有关联的设备设置已经更新。

SNMP

简单网络管理协议 (SNMP) 允许 CC-SG 向网络上的现有 SNMP 管理器推送 SNMP 陷阱（事件通知）。只有受到 SNMP 基础设施技能培训的 CC-SG 管理员才能配置 CC-SG 使用 SNMP。

CC-SG 还支持与第三方企业管理解决方案（如 HP OpenView）的 SNMP GET/SET 操作。要支持这些操作，必须提供 SNMP 代理识别符信息，例如以下 MIB-II 系统组对象：sysContact、sysName 和 sysLocation。详见 RFC 1213。这些标识符提供有关被管节点的联系、管理和位置信息。

MIB 文件

由于 CC-SG 推送自己的一套 Raritan 陷阱，必须使用包含 Raritan SNMP 陷阱定义的自定义 MIB 文件来更新所有的 SNMP 管理器。请参阅**附录 D：SNMP 陷阱**。这个自定义 MIB 文件位于 CC-SG 设备附带的 CD 上，也从 **http://www.raritan.com/support** 的“固件升级”位置下载。

在 CC-SG 中配置 SNMP

1. 从“管理”菜单中，单击“配置”。出现“配置管理器”屏幕。
2. 单击“SNMP”选项卡。

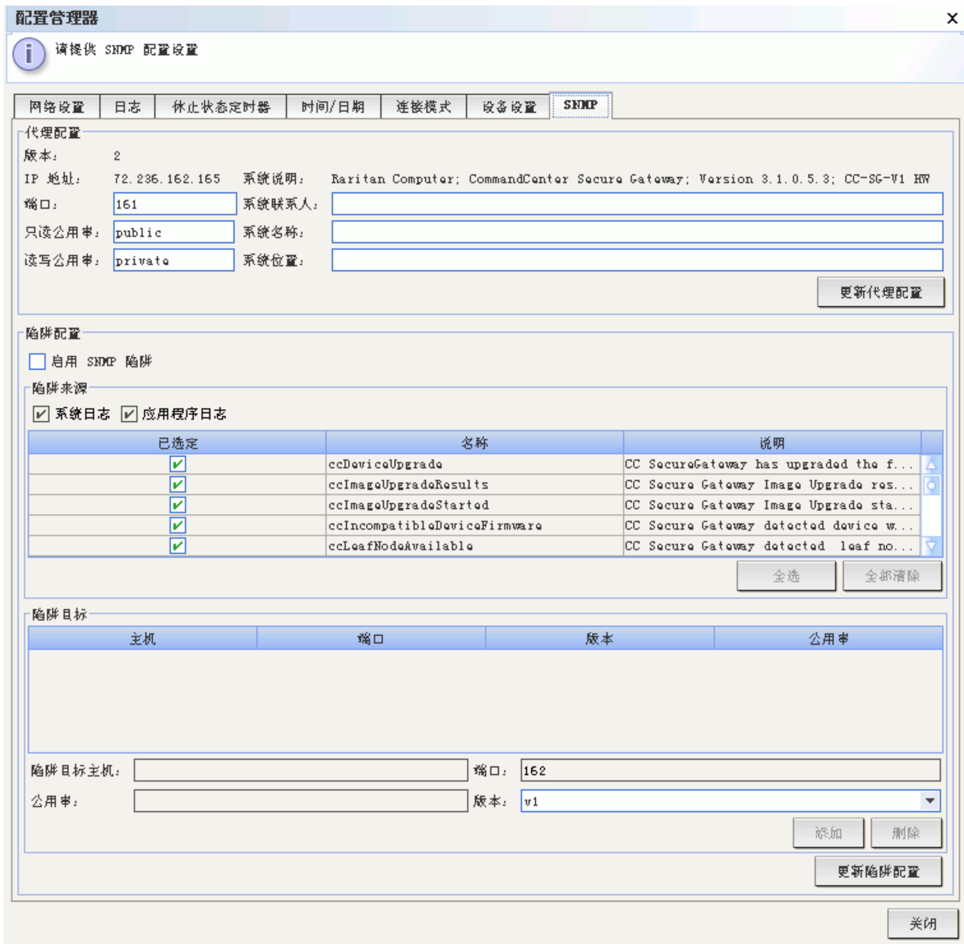


图 162 配置设置设备设置屏幕

3. 要将 CC-SG 上运行的 SNMP 代理标识为第三方企业管理解决方案，请在“代理配置”下面提供代理信息。键入代理的“端口”（默认为 161）。键入“只读公用串”字符串（默认值为“**public**”）、“读写公用串”字符串（默认值为“**private**”）。允许多个团体字符串，用逗号隔开。键入“系统联系人”、“系统名称”和“系统位置”提供有关被管节点的信息。
4. 单击“更新代理配置”保存 SNMP 代理标识符信息。
5. 在“陷阱配置”下面，选中“启用 SNMP 陷阱”框以启用从 CC-SG 向 SNMP 主机发送 SNMP 陷阱。
6. 选中想要 CC-SG 推送到 SNMP 主机的陷阱前面的框：
   在“陷阱来源”下面有一个 SNMP 陷阱列表，分成两类：“系统日志”陷阱：包括 CC 设备本身状态的通知，例如硬盘故障；“应用程序日志”陷阱：CC 应用程序中事件产生的通知，例如对用户帐户的修改。要启用按类型的陷阱，选中“系统日志”和“应用程

序日志”框。对于单个的陷阱，可选中其对应的复选框来启用或禁用，使用“全选”和“全部清除”可启用全部陷阱或清除所有复选框。有关提供的 SNMP 陷阱列表，参见 MIB 文件。详情参阅 **MIB 文件**。

7. 在“陷阱目标”面板内，键入 SNMP 主机使用的“陷阱目标主机”IP 地址和“端口”号。默认端口为 162。
8. 在“陷阱目标”面板内，键入 SNMP 主机使用的“公用串”字符串和“版本”（**v1** 或 **v2**）。
9. 单击“添加”将目标主机添加到已配置主机列表内。要从列表中删除主机，请选择该主机并单击“删除”。此列表中可以设置的管理器数量没有限制。
10. 配置 SNMP 陷阱及其目标后，单击“更新陷阱配置”。

群集配置

一个 CC-SG 群集使用两个 CC-SG 节点，一个主用一个备用，在主用 CC-SG 节点失效时可实现备份安全。两个节点共享活动用户和活动连接的数据，所有状态数据在两个节点之间复制。一个群集中的主用和备用节点必须运行同一版本的软件。如果用户不定义，CC-SG 将向每个群集节点分配默认名称。

CC-SG 群集中的设备必须知道主用 CC-SG 节点的 IP，才能向主用节点通知状态改变事件。如果主用节点失效，备用节点立即承担主用节点的所有功能。这需要初始化 CC-SG 应用程序和用户会话，主用 CC-SG 节点上发起的所有当前会话将会终止。主用 CC-SG 设备上连接的设备将发现主用节点不再响应，于是响应由备用节点发出的请求。

注：在群集配置中，只有主用 CC-SG 与 CC-NOC 进行通信。一旦 CC-SG 成为主用，将向 CC- NOC 发送其 IP 地址以及备用 CC-SG 的 IP 地址。

创建群集

出现故障切换时，管理员应向所有 CC-SG 用户发送一封电子邮件，通知他们使用新的主用 CC-SG 节点的 IP 地址。

重要说明：在设置群集配置之前，建议在两个节点上备份配置。

注：CC-SG 必须以“主用/备用”模式运行其网络端口，才能用于群集。群集将不会使用“活动/活动”配置。详情参见本章中的“网络配置”。

设置主用 CC-SG 节点

1. 从“管理”菜单中，单击“群集配置”。出现“群集配置”屏幕。
2. 单击“发现 CommandCenter”在当前使用的同一个子网内扫描和发现所有 CC-SG 设备。或者可以通过在窗口底部的“CommandCenter 地址”内指定 IP 地址，然后单击“添加 CommandCenter”，即可从其它子网添加 CC-SG。

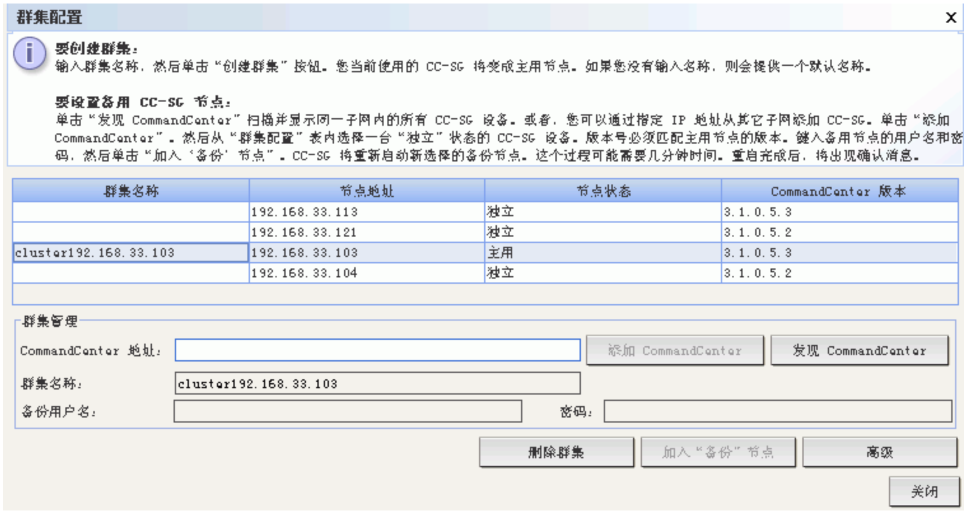


图 163 群集配置屏幕

3. 在“群集名称”内键入此群集的名称。如果现在不提供名称，在创建群集时将会提供一个默认名称，例如 cluster192.168.51.124。
4. 单击“创建群集”。
5. 当提示是否继续时，单击“是”。当前的使用的 CC-SG 将变为主用节点，如果以前没有在“群集名称”字段中输入名称，则会提供一个默认名称。

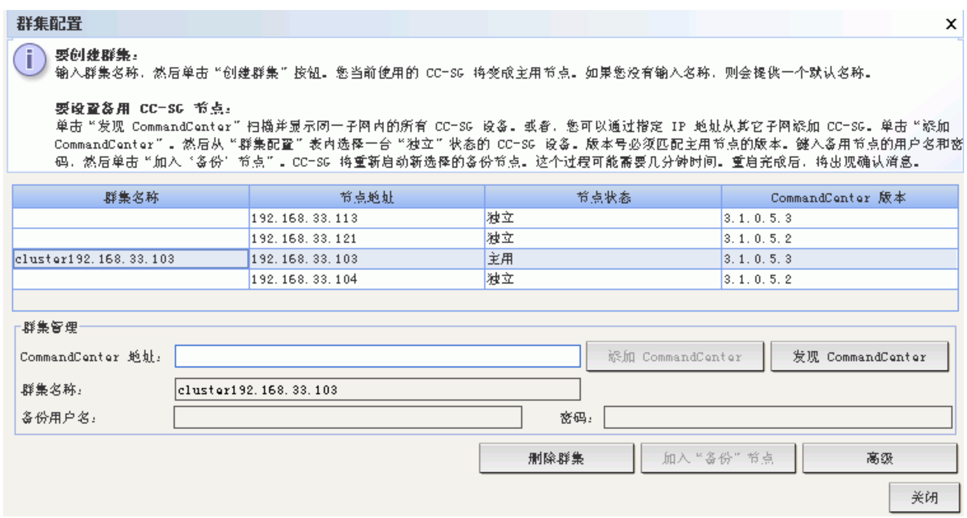


图 164 群集配置——主用节点设置

设置备用 CC-SG 节点

1. 单击“发现 CommandCenter”在当前使用的同一个子网内扫描和发现所有 CC-SG 设备。或者可以通过在窗口底部的“CommandCenter 地址”内指定 IP 地址，即从其它子网添加 CC-SG。单击“添加 CommandCenter”。

注：从其它子网或网络中添加备份 CC-SG，可避免受到单个网络或物理位置问题的影响。

2. 要添加备份节点或备份 CC-SG 节点，从“群集配置”表内选择状态为“单机”的 CC-SG 设备。版本号必须与主用节点的版本相同。
3. 在“备份用户名”和“密码”字段中为备份节点键入有效的用户名和密码。
4. 单击“加入‘备份’节点”。
5. 出现一条确认消息。单击“是”将备用状态分配到所选节点，或单击“否”取消。

重要事项！一旦开始加入过程后，不要在 CC-SG 中执行其它任何功能，指导加入过程完成为止，如下面第 6 步中所述。

6. 单击“是”以后，CC-SG 将重新启动新选择的备份节点。这个过程可能需要几分钟。重启完成后，屏幕上会出现一条确认消息。
7. 从“管理”菜单中，单击“群集配置”查看更新的“群集配置”表。

注：如果主用和备用节点彼此失去通信，备用节点将承担主用节点的角色。连接恢复后，将可能有两个主用节点。这时应删除一个主用节点，将其复位为备用节点。

删除备用 CC-SG 节点

1. 要从 CC-SG 设备中删除“备用节点”状态并将此状态重新分配给配置中的其它设备，请在“群集配置”表内选择备用 CC-SG 节点，然后单击“删除‘备份’节点”。
2. 出现确认消息后，单击“是”删除备用节点状态，或单击“否”取消。

注：单击“删除‘备份’节点”将删除备用节点的名称。不会从配置中删除备用 CC-SG 设备。

删除主用 CC-SG 节点

1. 要从 CC-SG 设备中删除“主用节点”状态并将此状态重新分配给配置中的其它设备，请在“群集配置”表内选择主用 CC-SG 节点，然后单击“删除群集”。
2. 出现确认消息后，单击“是”删除主用节点状态，或单击“否”取消。

注：单击“删除群集”并不会从配置中删除主用 CC-SG 设备，而仅是删除“主用节点”的分配。只有不存在备份节点时，“删除群集”才可用。

恢复故障 CC-SG 节点

当一个节点故障并发生故障切换时，故障的节点将恢复为“等待”状态。

1. 在“群集配置”表内选择“等待”的节点。
2. 单击“加入‘等待’节点”可将其添加为备份节点。
3. 出现一条确认消息。单击“是”将备用状态分配到所选节点，或单击“否”取消。如果单击“是”，则需要等待备用节点重新启动，就像“加入‘备份’节点”一样。

注：节点处于“等待”状态后，可以“单机”模式或“备份”模式启动。

设置高级设置

要配置群集配置的高级设置：

1. 选择所创建的主用节点。
2. 单击“高级”。出现“高级设置”窗口。

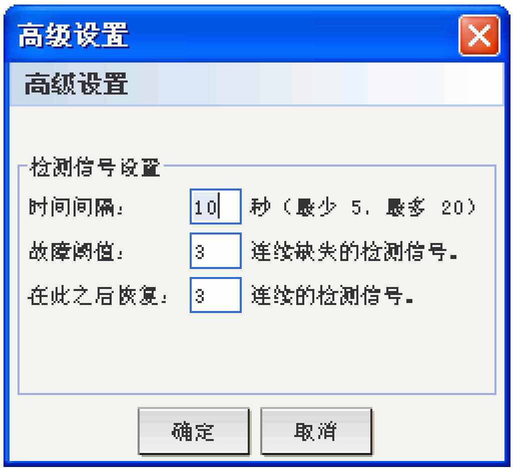


图 165 群集配置高级设置

3. 对于“时间间隔”，输入 CC-SG 应多久一次检查与另一节点连接。

注：如果“时间间隔”设置较小，则检测信号的检查所产生的网络流量就会增加。同时，群集中节点位置彼此较远时可能需要设置较高的间隔。

4. 对于“故障阈值”，输入在 CC-SG 节点被认为故障之前需要连续传递的无响应检测信号个数。
5. 对于“在此之后恢复”，输入在故障的连接被认为恢复之前需要成功返回的连续检测信号个数。
6. 单击“确定”保存设置。

注：在群集配置上禁用更改时区。

配置安全性

“安全管理器”用于管理 CC-SG 如何提供到用户的访问。使用“安全管理器”可配置认证方法、SSL 访问、严格密码规则、锁定规则、登录门户、证书和访问控制列表。

远程认证

有关配置远程认证服务器的详细指导说明，请参阅**第 9 章：配置远程认证**。

安全客户端连接

在“安全管理器”中，可为 CC-SG 上的客户端连接配置安全设置。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕。
2. 单击“常规”选项卡。



图 166 安全客户端连接

3. 如果想要使用到 CC-SG 的 AES 加密连接，选中“客户端和服务器之间需要 AES 加密”复选框。在“密钥长度”字段中键入要使用的加密密钥长度。默认密钥长度 128。
4. 在“SSH 服务器端口”字段中键入用于通过 SSH 访问 CC-SG 的端口号。详见本章后面的“CC-SG 的 SSH 访问”。
5. 单击“HTTP”或“HTTP/SSL”单选按钮选择客户端在连接 CC-SG 时要使用的浏览器连接协议。必须重新启动 CC-SG 让设置的更改生效。
6. 单击“更新”保存更改。

登录设置

“登录设置”允许配置“严格密码设置”和“锁定设置”。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕。
2. 单击“登录设置”选项卡。

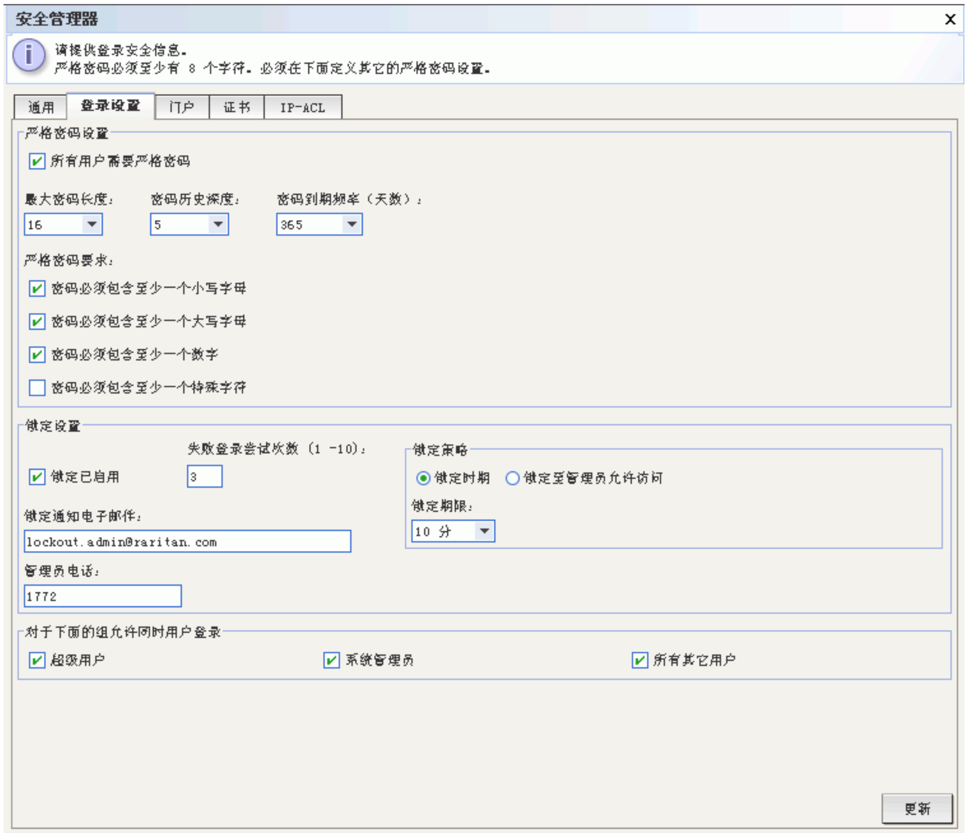


图 167 登录设置

严格密码设置

严格密码规则要求用户在创建密码时要遵循严格的指导原则，让密码更难以猜测，因此理论上就更安全。默认情况下 CC-SG 中不启用严格密码。要使用严格密码，管理员应首先选中“所有用户需要严格密码”。

注：对于 CC 超级用户，总是要求使用包含所有严格密码要求的严格密码。

一旦启用，管理员即可在“严格密码”设置中编辑字段来自定义密码规则。在最低的情况下，所有的严格密码必须按照以下标准配置：

- **最小密码长度** – 所有密码必须包含最小个数的字符。单击该下拉菜单选择最小密码长度。
- **密码历史深度** – 单击下拉菜单，选择历史中保存多少个以前的密码。要求选择新密码时，用户将无法再次使用历史中的密码。例如，如果“密码历史”设为 5，则用户不能重复使用他们的最后 5 个密码。
- **密码到期频率** – 所有密码要在一定的天数后到期。单击该下拉菜单选择密码保持有效的天数。密码到期后，将要求用户在下次登录时选择新密码。

此外，用户名和密码中任何四个相邻字符不能相同。

在严格密码要求下，管理员可配置密码规则来要求几条附加项：

- 密码必须包含至少一个小写字母。
- 密码必须包含至少一个大写字母。
- 密码必须包含至少一个数字。
- 密码必须包含至少一个特殊字符（例如感叹号或 & 号）。

配置严格密码完成以后，单击“更新”保存设置。所有选择的规则都是累积的，也就是说，所有密码必须满足管理员所配置的每一个规则。配置严格密码规则以后，所有将来的密码都要满足这些标准，并且如果新的标准要比以前的标准严格，则所有用户在下次登录时都要更改其密码。强制密码规则仅应用于本地存储的用户配置文件。在认证服务器上的密码规则必须由认证服务器自己管理。

Raritan 建议更改严格密码时，使用“当日消息”功能为用户提供提前通知，并告知新标准的内容。

锁定设置

在指定次数的失败登录尝试后，管理员可锁定 CC-SG、CC-NOC 用户与 SSH 用户。这项功能适用于由 CC-SG 本地认证和授权的用户，不适用于由外部服务器远程认证的用户。详情参阅**第 9 章：配置远程认证**。因用户许可不足而失败的登录尝试则不适用。

---

*注：默认情况下，**admin** 帐户三次登录尝试失败后将被锁定五分钟。对于 **admin**，锁定前后失败登录尝试次数不能配置。*

要配置用户锁定：

1. 选中“锁定已启用”。
2. 用户锁定前失败登录尝试的默认次数为 3。可输入 1 到 10 之间的数字更改此值。
3. 选择一个“锁定策略”：
   a. 如果选择“锁定时期”，则指定一个时间周期（分钟），用户将被锁定这段时间后才能再次登录。默认时间为 5 分钟，但可指定 1 到 1440 分钟（24 小时）之间的任何数字。时间到后，用户即可再次登录。在锁定期间的任何时间，管理员可越过此值，允许用户重新登录 CC-SG。
   b. 如果选择“锁定至管理员允许访问”，表示用户将被锁定直到管理员允许其重新登录为止。要锁定一个用户，详情参阅**第 10 章：生成报告**。
4. 在“锁定通知电子邮件”中键入一个电子邮件地址，向该地址发送通知，告知接收人已发生锁定。如果此字段为空，则不发送通知。
5. 如果需要联络管理员，则在“管理员电话”中键入电话号码。
6. 单击“更新”保存配置设置。

允许每个用户名同时登录

这些设置允许使用同一个用户在 CC-SG 上同时存在多个会话。

1. 如果要允许 admin 帐户在 CC-SG 上有多个同时连接，则选中“超级用户”。
2. 如果要允许“系统管理员”用户组中的帐户同时登录，则选中“系统管理员”。
3. 如果要允许所有其它帐户同时登录，则选中“其他用户”。

门户

门户设置允许管理员配置徽标和访问协议，在用户访问客户端时提供问候语。要访问门户设置：

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕。
2. 单击“门户”选项卡。

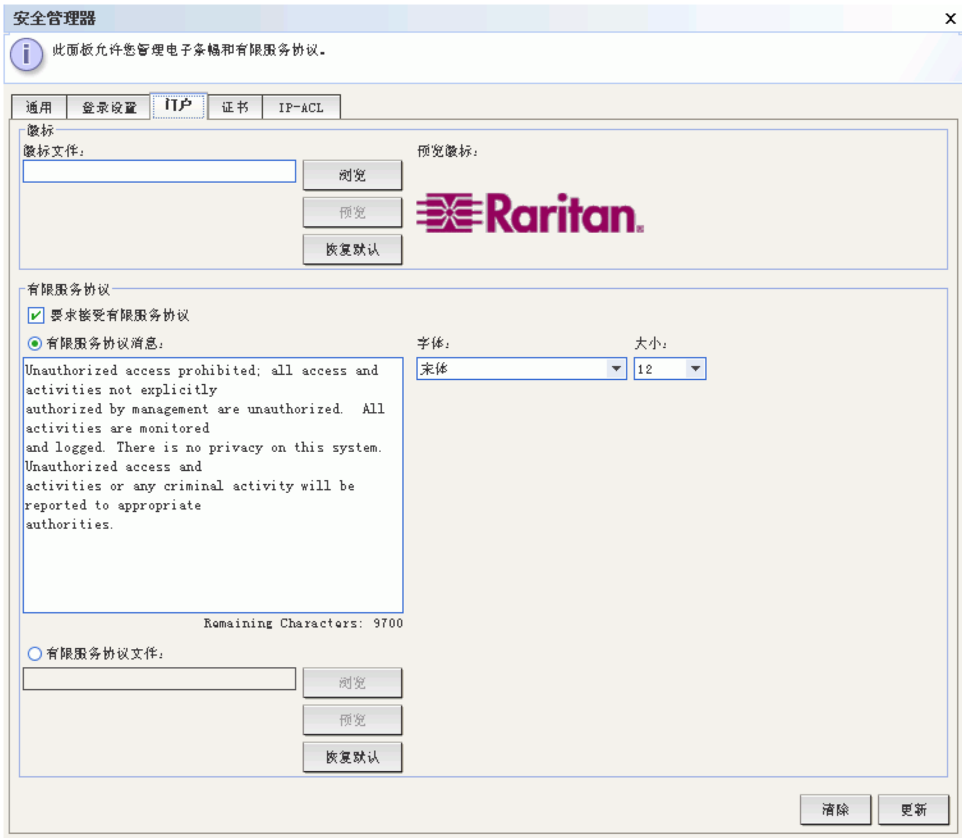


图 168 门户设置

徽标

可将一个小的图形文件上载到 CC-SG 作为登录页面的条幅。徽标的最大大小为 998 X 170 像素。要上载徽标：

1. 在“门户”选项卡的“徽标”区域内，单击“浏览”。出现“打开”对话框。
2. 在对话框中选择要用作徽标的图形文件，然后单击“打开”。
3. 如果需要，单击“预览”预览徽标。所选的图形文件将在右侧显示。
4. 单击“更新”将徽标更改保存到 CC-SG。

有限服务协议

可配置一条消息显示在登录屏幕上登录字段的左边。这可以用作有限服务协议，或者作为用户访问 CC-SG 时要同意的声明。用户接受有限服务协议将在日志文件和审计跟踪报告中记录。

1. 单击“要求接受有限服务协议”即要求用户在登录屏幕上选中协议框，然后才允许其输入登录信息。

2. 如果要直接输入条幅文本，则选择“有限服务协议消息”。
   a. 在提供的文本字段中添加协议消息。文本消息的最大长度为 10000 个字符。
   b. 单击“字体”下拉菜单，选择显示消息的字体。
   c. 单击“大小”下拉菜单，选择显示消息的字体大小。

   如果要从文本文件 (.TXT) 上载一条消息，则选择“有限服务协议消息”。
   d. 单击“浏览”。出现对话窗口。
   e. 在对话窗口中，选择要使用的含有消息的文本文件，然后单击“打开”。文本消息的最大长度为 10000 个字符。
   f. 如果要预览文件中包含的文本，单击“预览”。将在上面的条幅消息字段中显示。
3. 单击“更新”将有限服务条幅更改保存到 CC-SG。

   更新徽标和有限服务协议设置后，将在下次用户访问客户端时显示在登录屏幕上。



图 169 带有有限服务协议的登录门户

证书

此窗口中的选项可用来生成证书签名的请求（也称为 CSR 或证书请求）。CSR 是申请者发往证书机构的消息，用于申请数字身份证书。创建 CSR 之前，申请者首先生成一个密钥对，将私有密钥保密。CSR 包含识别申请者的信息（例如对于 X.509 证书为目录名称），以及申请者所选择的公共密钥。

注：屏幕底部的按钮将从“导出”变成“导入”，然后变成“生成”，取决于所选哪个证书选项。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕。
2. 单击“证书”选项卡。

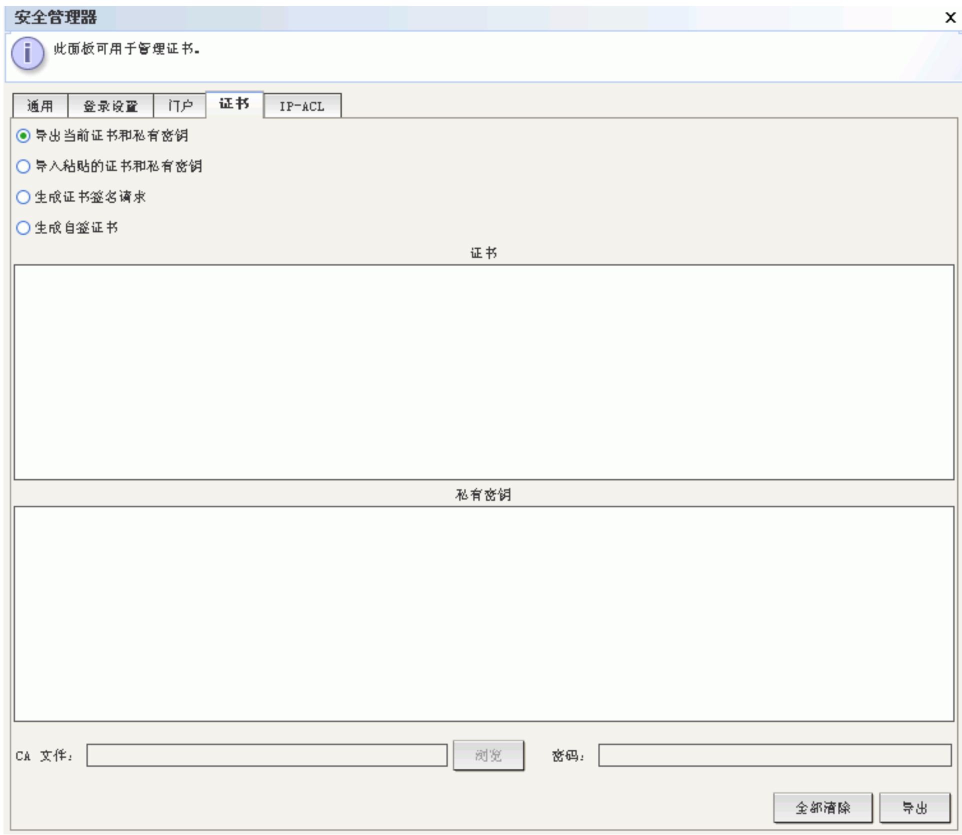


图 170 安全管理器证书屏幕

导出当前证书和私有密钥

单击“导出当前证书和私有密钥”。证书显示在“证书”面板内，私有密钥显示在“私有密钥”面板内。复制“证书”和“私有密钥”的文本，单击“导出”提交。

生成自签名证书

下面解释如何在 CC-SG 上生成 CSR 和私有密钥。CSR 将提交给证书服务器，证书服务器将会签发签名证书。根证书也将从证书服务器导出，保存在文件中。然后即可导入签名证书、根证书和私有密钥。

1. 单击“生成证书签名请求”并单击“生成”。出现“生成证书签名请求”窗口。
2. 在字段中键入 CSR 请求的数据。

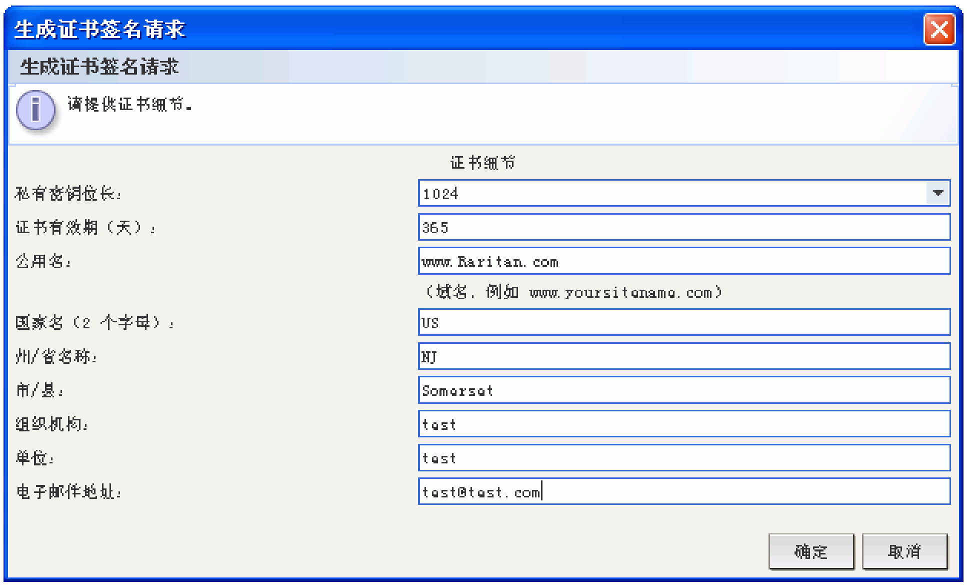


图 171 生成证书签名请求屏幕

3. 单击“确定”生成 CSR，或单击“取消”退出窗口。CSR 和私有密钥出现在“证书”屏幕中的对应字段内。



图 172 生成的证书请求

4. 使用 ASCII 编辑器（例如记事本），复制 CSR 并粘贴到文件中，保存为 .cer 文件。
5. 使用 ASCII 编辑器（例如记事本），复制私有密钥并粘贴到文件中，保存为文本文件。

6. 将第 4 步中生成的 CSR 文件（**.cer**）提交给证书服务器，以从服务器获得签名证书。
7. 从证书服务器下载或导出根证书，保存为 .cer 文件。此证书不同于下面的步骤中由证书服务器签发的签名证书。
8. 从证书服务器收到签名证书后，单击“导入粘贴的证书和私有密钥”。
9. 复制签名证书并粘贴到“证书请求”字段。将以前保存的私有密钥粘贴到“私有密钥”字段。
10. 单击“CA 文件：”旁边的“浏览”，选择在第 6 步中保存的证书文件。
11. 如果 CSR 由 CC-SG 生成，在“密码”字段中键入“raritan”。如果其它应用程序生成 CSR，请使用该应用程序的密码。

注：如果导入的证书由根和子根 CA（证书机构）签名，则仅使用根或子根将会失败。要解决这个问题，请复制根以及子根证书并粘贴到一个文件中，然后将其导入。

生成自签证书请求

单击“生成自签证书”选项按钮，然后单击“生成”。出现“生成自签名证书”窗口。在字段中键入自签证书所需的数据。单击“确定”生成证书，或单击“取消”退出窗口。在“证书”屏幕中的对应字段内以加密的形式显示证书和私有密钥。

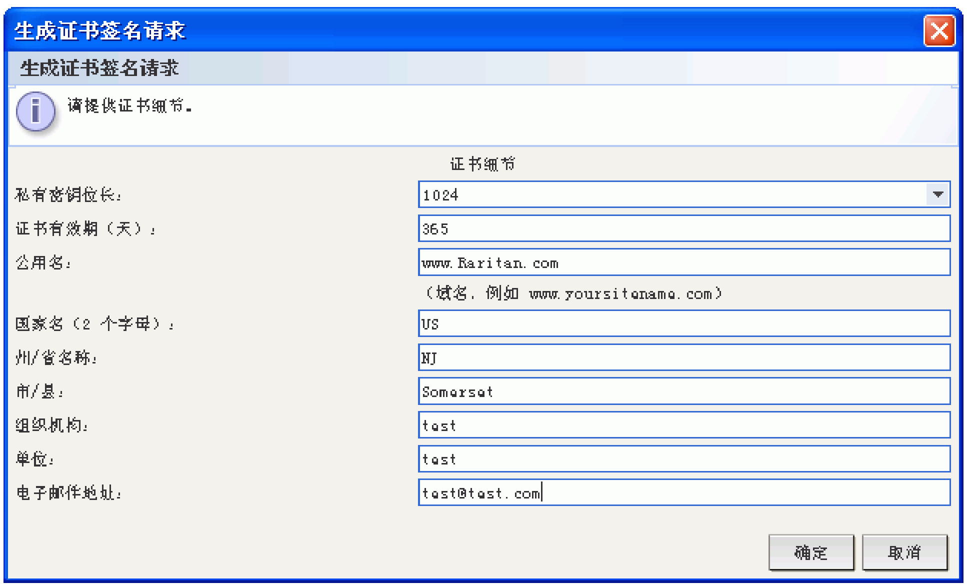


图 173 生成自签证书窗口

IP-ACL

此功能将基于 IP 地址限制到 CC-SG 的访问。通过输入 IP 地址范围、所应用的组以及拒绝或允许权限，指定一个 IP 访问控制列表（IP-ACL）。

1. 从“管理”菜单中，单击“安全”。出现“安全管理器”屏幕。
2. 单击“IP-ACL”选项卡。

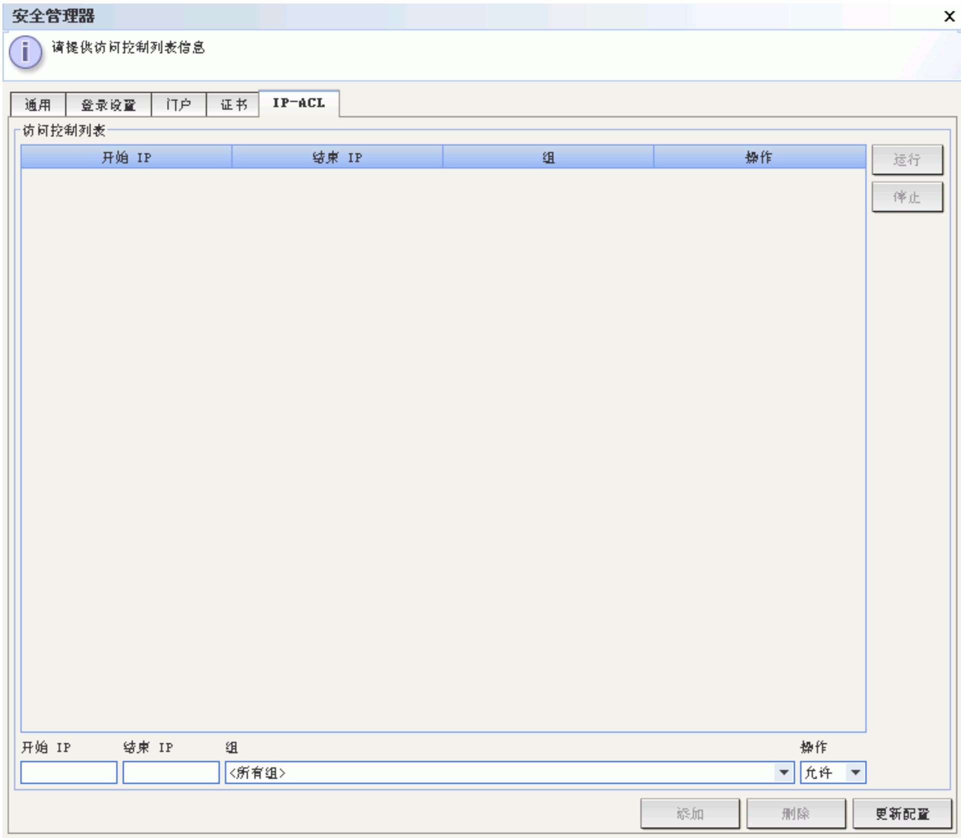


图 174 安全管理器 IP-ACL 屏幕

3. 要更改“访问控制列表”内行项目的顺序，选择该行项目，然后单击“向上”或“向下”。将会根据适用的第一条规则（从上至下）对连接的用户进行允许或拒绝。
4. 要向列表中添加新项目，在“开始 IP”字段中键入开始 IP 值，在“结束 IP”字段中输入结束 IP 值，即可指定应用规则的范围。
5. 单击“组”下拉箭头并选择要应用规则的组。
6. 单击“操作”下拉箭头并从列表中选择“允许”或“拒绝”对 IP 范围的组访问。
7. 单击“添加”将新规则添加到“访问控制列表”。
8. 要删除任何行项目，选择并单击“删除”。
9. 单击“更新配置”使用新的访问控制规则来更新系统。

通知管理器

“通知管理器”用来配置外部 SMTP 服务器，从而可从 CC-SG 发送通知。通知用于通过电子邮件发送已经计划的报告、用户被锁定的报告、计划任务的失败或成功状态。详情参阅本章后面的“任务管理器”部分。配置 SMTP 服务器后，可选择向接收人发送一封测试电子邮件，并向接收人通知测试的结果。

要配置外部 SMTP 服务器：

1. 从“管理”菜单中，单击“通知”。出现“通知管理器”屏幕。



图 175 通知管理器

2. 选中“启用 SMTP 通知”复选框。
3. 在“SMTP 主机”字段内键入 SMTP 主机。对于主机名规则，参见**第 1 章：简介**中的“**术语/缩略语**”。
4. 在“SMTP 端口号”字段内键入有效的 SMTP 端口号。
5. 在“帐户名称”字段中键入用于登录 SMTP 服务器的有效帐户名称。
6. 在“密码”和“重新输入密码”字段中键入帐户名的密码。
7. 在“从”字段中键入有效的电子邮件地址，用于标识从 CC-SG 发出的消息。
8. 在“发送重试次数”字段中键入发送进程失败后重复发送电子邮件的次数。
9. 在“发送重试间隔（分钟）”字段中键入重复发送尝试之间经过的分钟数，范围是 0-60。
10. 如果要通过的安全套接字层 (SSL) 安全发送电子邮件，则选中“使用 SSL”。
11. 单击“测试配置”向指定的 SMTP 帐户发送一封测试电子邮件。检查以确认邮件是否到达。
12. 单击“更新配置”保存更改。

任务管理器

“任务管理器”用于按每天、每周、每月或每年计划 CC-SG 任务。可计划任务仅运行一次，或按指定的时间间隔在每周的指定一天周期性地运行，例如在每三周的周五计划设备备份，或每周一将特殊报告通过电子邮件发送给一个或多个接收人。

注：“任务管理器”使用在 CC-SG 上设置的服务器时间用于计划，而非在客户端 PC 上设置的时间。服务器时间显示在每个 CC-SG 屏幕的右上角。

任务类型

可计划以下这些任务：

- 备份设备配置（单个设备或设备组）
- 恢复设备配置（不适用于设备组）
- 复制设备配置（单个设备或设备组）
- 升级设备固件（单个设备或设备组）。注意在计划任务前固件首先要可用。
- 备份 CC-SG
- 重新启动设备（不适用于设备组）
- 出口端口电源管理（开机/关机/循环出口端口）
- 生成所有报告（HTML 或 CSV 格式）
- 清理日志

计划顺序任务

可能需要顺序计划任务以确认实际执行的期望行为。例如，可能需要为给定的设备组计划一个“升级设备固件”任务，然后立即计划一个“资产管理报告”任务，以确认是否升级正确的固件版本。

电子邮件通知

在完成一个任务后，将向指定的接收人发送一条电子邮件消息。在“通知管理器”中可指定在何处以及如何发送电子邮件，例如是否通过 SSL 安全发送。详情参阅本章前面的“通知管理器”部分。

计划报告

计划的报告通过电子邮件发送给指定的接收人。

所有状态为“完成”的报告将在 CC-SG 上存储 30 天，可在“报告”菜单下选择“计划报告”以 HTML 格式查看这些报告。详情参见**第 10 章：生成报告中的“计划报告”**。

创建新任务

要计划新任务：

1. 从“管理”菜单中，单击“任务”。出现“任务管理器”屏幕。

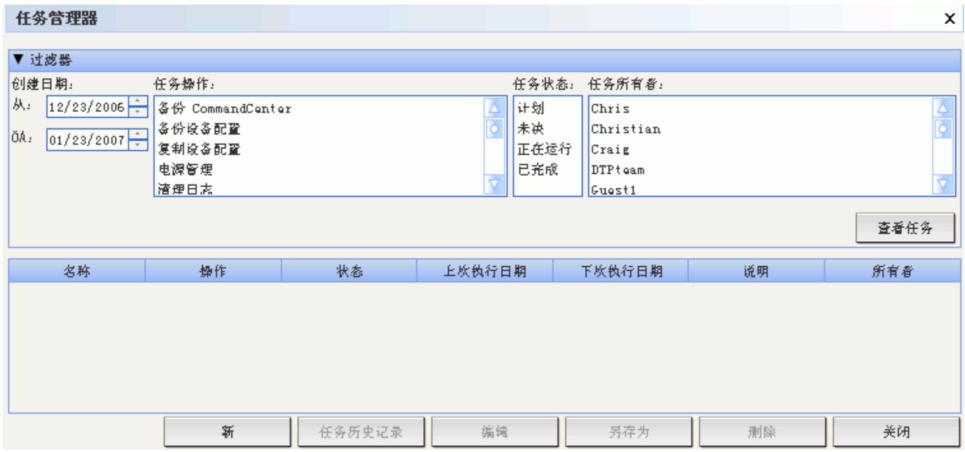


图 176 任务管理器

2. 单击“新建”。
3. 在“主”选项卡内，键入任务的名称（1-32 个字符，字母数字字符或下划线，无空格）和说明。
4. 单击“任务数据”选项卡。
5. 单击“任务操作”下拉菜单，从列表中选择要计划的任务，例如“升级设备固件”。注意根据所选的任务，字段需要的数据会有所不同。
6. 单击“重复”选项卡。
7. 在“周期”字段内，单击要重复执行计划任务时段所对应的单选按钮。
   - **一次：**使用上下箭头选择任务开始的“开始时间”。
   - **定期：**使用上下箭头选择任务开始的“开始时间”。在“重复计数”字段中键入执行任务的次数。在“重复间隔”字段中键入重复之间应经过的时间。单击下拉菜单，从列表中选择时间单位。
   - **每天：**如果要每周 7 天重复任务，则单击“每天”旁边的单选按钮。如果要从周一到周五每天重复任务，则单击“每个工作日”旁边的单选按钮。
   - **每周：**使用上下箭头选择任务执行之间经过的周数，然后选中在每个运行周内应重复任务的天旁边的复选框。
   - **每月：**在“天”字段中键入应执行任务的日期，然后选中指定日期上应重复任务所在月份旁边的复选框。
   - **每年：**单击下拉菜单，从列表中选择执行任务的月份。使用上下箭头选择执行任务当天所在的月份。
8. 从“每天”、“每周”、“每月”和“每年”任务中，必须在“重复范围”部分内为任务添加开始和结束时间。使用上下箭头选择“开始时间”和“开始日期”。如果任务应按照指定无限重复，则单击“无结束日期”旁边的单选按钮。或者，单击“结束日期”旁边的单选按钮，然后使用上下箭头选择停止任务重复的日期。
9. 单击“重试”选项卡。
10. 如果任务失败，CC-SG 可根据在“重试”选项卡内指定的稍后时间重新尝试任务。在“重试计数”字段中键入 CC-SG 应重新尝试执行任务的次数。在“重试间隔”字段中键入重试之间应经过的时间。单击下拉菜单，从列表中选择时间单位。

重要说明：如果计划一个任务来升级 SX 或 KX 设备，请将“重试间隔”设为 20 分钟以上，因为成功升级这些设备需要大约 20 分钟的时间。

11. 单击“通知”选项卡。
12. 可指定电子邮件地址用于在任务成功或失败时发送通知。默认情况下，将使用当前登录用户的电子邮件地址。使用电子邮件地址在“用户配置文件”中配置。详情参见第 7 章：添加和管理用户和用户组。要添加其它电子邮件地址，单击“添加”，在出现的窗口中键入电子邮件地址，然后单击“确定”。默认情况下，如果任务成功即发送电子邮件。要将失败任务通知接收人，单击“失败时”复选框。
13. 单击“确定”保存任务。

查看任务、任务细节和任务历史

要查看任务：

1. 从“管理”菜单中，单击“任务”。出现“任务管理器”屏幕。
2. 要搜索任务，使用上下按钮选择要搜索的日期范围。从每个列表中，可选择一个或多个（按住 Ctrl 键单击）任务、状态或所有者进一步过滤列表。单击“查看任务”可查看任务列表。

- 要删除任务，请选择该任务，然后单击“删除”。

注：无法删除当前正在运行的任务。

- 要查看任务历史，选择一个任务并单击“任务历史”。
- 要查看任务细节，双击任务即可。
- 要更改计划任务，请选择该任务，然后单击“编辑”打开“编辑任务”窗口。根据需要更改任务参数，然后单击“更新”。有关选项卡描述，请参阅本章前面的“创建新任务”部分。
- 要基于以前配置的任务创建新任务，选择要复制的任务，然后单击“另存为”打开“另存为任务”窗口。选项卡中将填充以前配置任务的信息。根据需要更改任务参数，然后单击“更新”。有关选项卡描述，请参阅本章前面的“创建新任务”部分。

注：如果任务被更改或更新，它以前的历史将不再适用，“上次执行日期”将变空。

CommandCenter NOC

将 CommandCenter NOC (CC-NOC) 添加到系统将能够为串行和 KVM 目标系统提供监视、报告和警告服务，从而扩展目标管理功能。有关安装和操作 CC-NOC 设备的详细指导说明，请参阅 Raritan 的 CommandCenter NOC 文档。

重要说明：在下面的过程中会生成通行码。需要将这些通行码提供给 CC-NOC 管理员，由管理员在五分钟内将其配置到 CC-NOC。避免通过电子邮件或其它电子手段发送通行码，避免可能被自动系统截获。两个互信方可通过电话或书面方式交换代码，也能较好地防止自动化截获问题。

添加 CC-NOC

注：要创建一条有效链接，CC-NOC 与 CC-SG 上的时间设置应同步。获得同步的最好办法是使用共同的 NTP（网络时间协议）服务器。为此，需要为 CC-NOC 和 CC-SG 配置使用一台 NTP 服务器。

1. 在“访问”菜单上，单击“CC-NOC 配置”。出现“CC-NOC 配置”屏幕。
2. 单击“添加”。出现“添加 CC-NOC 配置”屏幕。
3. 选择要添加的 CC-NOC 软件版本，然后单击“下一步”。版本 5.1 的集成功能相对 5.2 及更高版本较少，仅需要添加名称和 IP 地址。有关 CC-NOC 5.1 的详细信息，请访问 **www.raritan.com/support**。单击“产品文档”，然后单击“CommandCenter NOC”。

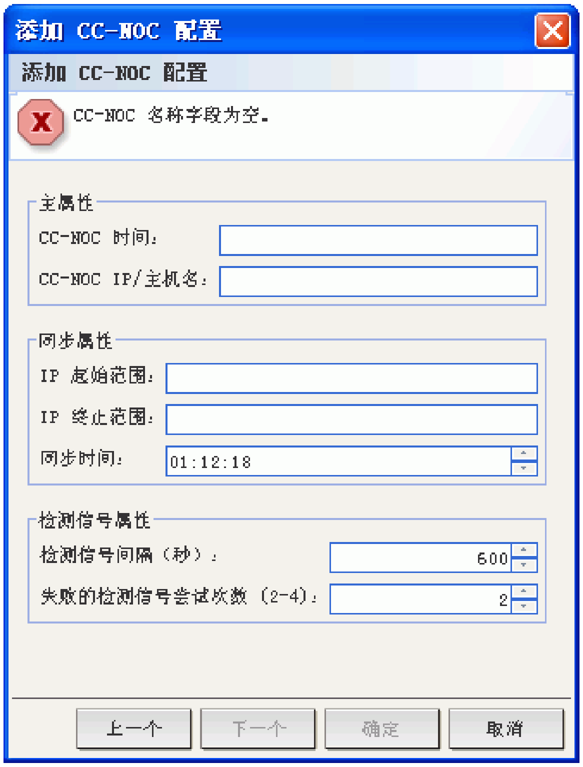


图 177 添加 CC-NOC 配置屏幕

4. 在“名称”字段内键入 CC-NOC 的描述性名称。最长为 50 个字母数字字符。
5. 在“CC-NOC IP/主机名”字段中键入 CC-NOC 的 IP 地址或主机名。这是必填字段。对于主机名规则，参见**第 1 章：简介**中的“**术语/缩略语**”。

6. 要检索 CC-NOC 数据库内的有关目标的每日信息，请在“IP 起始范围”和“IP 终止范围”字段中键入发现范围。此 IP 范围代表 CC-SG 感兴趣的地址范围，指示 CC-NOC 将这些设备的事件发送给 CC-SG。此范围与在 CC-NOC 中配置的发现范围有关。详见 Raritan 的《CommandCenter NOC 管理员指南》。键入范围，牢记以下规则：

IP 地址范围	说明
如果此处输入的 CC-SG 范围是在 CC-NOC 中配置范围的子网，	则 CC-NOC 返回此范围内所有已知目标设备信息。
如果此处输入的 CC-SG 范围包含在 CC-NOC 中配置范围的部分列表（交集非空），	则 CC-NOC 返回此相交范围内所有已知目标设备信息。
如果 CC-SG 范围是在 CC-NOC 中配置范围的超子集，	则 CC-NOC 返回此范围内所有已知目标设备信息。本质上，CC-NOC 返回在 CC-NOC 范围内定义的目标。
如果 CC-SG 范围与在 CC-NOC 中配置的范围不重叠，	则 CC-NOC 将不会返回任何目标设备信息。

要停止 CC-NOC 监视设备，可为“取消管理”。有关详细信息，请参阅《CommandCenter NOC 管理员指南》。

*注：使用 CC-NOC 同步报告查看 CC-SG 订阅的目标。此报告也显示 CC-NOC 所发现的任何新目标。详见**第 10 章：生成报告**的“CC-NOC 同步报告”。*

7. 指定一个“同步时间”计划何时从 CC-NOC 数据库内检索目标信息。被发现的设备被取消管理时将会刷新数据库。默认值为客户端机器上设置的当前时间。可能需要将同步计划在非高峰时间，使同步不会影响其它进程的性能。
8. 对于“检测信号间隔”，输入 CC-SG 多久（秒）向 CC-NOC 发送一次检测信号消息。这可确认 CC-NOC 是否依然运行且可用。默认值为 60 秒。有效范围是 30-120 秒。通常这不需要更改。
9. 对于“失败的检测信号尝试次数”，输入在 CC-NOC 节点被认为不可用之前需要连续传递的无响应检测信号个数。默认值为 2 个检测信号。有效范围是 2-4 个检测信号。通常这不需要更改。
10. 单击“下一步”。
11. 复制通行码并粘贴到 CC-NOC 字段中（如果您是 CC-NOC 管理员），或者将两个通行码提交给 CC-NOC 管理员。如《CommandCenter NOC 管理员指南》所述，CC-NOC 管理员然后将通行码输入 CC-NOC，将开始一次安全证书的交换。

重要说明：为了提高安全性，在 CC-SG 生成通行码后需要在五分钟内输入到 CC-NOC。这将使入侵者通过暴力破解攻击系统的机会降至最低。避免通过电子邮件或其它电子手段发送通行码，避免可能被自动系统截获。两个互信方可通过电话或书面方式交换代码，也能较好地防止自动化截获问题。

12. 证书交互过程完成后，即在 CC-SG 配置 CC-NOC 之间建立一条安全通道。CC-NOC 数据将被复制到 CC-SG。单击“确定”完成该过程。如果该过程在 5 分钟之内仍未完成，则会超时，数据不保存在 CC-SG 内，任何存储的证书将被删除。重新尝试这个过程——返回第 179 页“**添加 CC-NOC**”的第 1 步。

注：CommandCenter NOC 只能添加到单机或主用节点 CC-SG 服务器。

编辑 CC-NOC

1. 在“访问”菜单上，单击“CC-NOC 配置”。出现“CC-NOC 配置”屏幕。
2. 在列表中选中一个 CC-NOC 并单击“编辑”。出现“编辑 CC-NOC 配置”屏幕。
3. 根据需要更改配置。对于其它信息字段，请参阅上节**“添加 CC-NOC”**部分。

启动 CC-NOC

要从 CC-SG 启动 CC-NOC：

1. 在“访问”菜单上，单击“CC-NOC 配置”。
2. 在“CC-NOC 配置”屏幕上，选中一个可用的 CC-NOC。
3. 单击“启动”。这将连接到一个配置的 CC-NOC。

删除 CC-NOC

要在 CC-SG 中删除及取消注册 CC-NOC，请执行以下操作。

1. 在“访问”菜单上，单击“CC-NOC 配置”。出现“CC-NOC 配置”屏幕。
2. 选择要从 CC-SG 删除的 CC-NOC，然后单击“删除”。将提示您确认删除。
3. 单击“是”删除 CC-NOC。出现“CC-NOC 已成功删除”消息即确认 CC-NOC 已被删除。

至 CC-SG 的 SSH 访问

Secure Shell (SSH) 客户端（例如 Putty 或 OpenSSH 客户端）用于在 CC-SG 上访问至 SSH (v2) 服务器的命令行界面。仅通过 SSH 为管理设备和 CC-SG 本身提供 CC-SG 命令的子集。

SSH 客户端用户由 CC-SG 进行认证，其中现有的认证和授权策略应用到 SSH 客户端。提供给 SSH 客户机的命令是由 SSH 客户端用户所属的用户组权限决定的。

使用 SSH 访问 CC-SG 的管理员不能注销 CC 超级用户 SSH 用户，但可以注销所有其他 SSH 客户端用户，包括管理员。

要通过 SSH 访问 CC-SG：

1. 启动 SSH 客户端，例如 Putty。
2. 指定 CC-SG 的 IP 地址并指定端口 22，然后打开连接。可在“安全管理器”中配置 SSH 访问端口。详情参阅本章前面的“安全管理器”部分。
3. 出现提示后，使用 CC-SG 的用户名和密码登录。

4. 出现一个 Shell 提示符。键入 ls 显示所有可用的命令。可键入 **?** 或 **help** 显示键入所有命令的描述和格式。

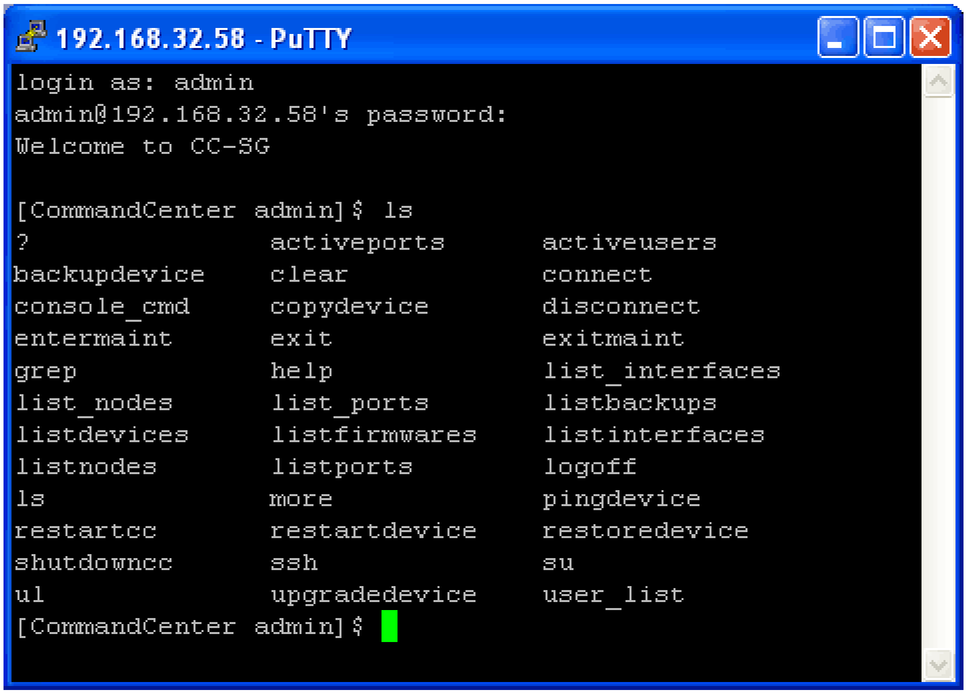


图 178 通过 SSH 的 CC-SG 命令

SSH 命令

下表介绍在 SSH 中所有可用的命令。需要在 CC-SG 中获得合适的权限才能访问各个命令。

命令说明
activeports 列出活动端口。
activeusers 列出活动用户。
backup device <[-host <host>] | [-id <device_id>]> backup_name [description] 备份设备配置。
clear 清除屏幕。
connect [-d <device_name>] [-e <escape_char>] <[-i <interface_id>] | [-n <port_name>] | [port_id]> 建立到串口的连接。如果 <port_name> 或 <device_name> 包含空格，则应用引号包括。
copydevice <[-b <backup_id>] | [source_device_host]> target_device_host 复制设备配置
disconnect <[-u <username>] [-p <port_id>] [-id <connection_id>]> 关闭端口连接。
entermaint minutes [message] 将 CC-SG 置于维护模式。
exitmaint 退出 CommandCenter 的维护模式。

grep search_term
从管道输出流中搜索文本。

help
查看帮助屏幕。

listbackups <[-id <device_id>] | [host]>
列出可用的设备配置备份。

listdevices
列出可用设备。

listfirmwares [[-id <device_id>] | [host]]
列出可用于升级的固件版本。

listinterfaces [-id <node_id>]
列出所有接口。

listnodes
列出所有节点。

listports [[-id <device_id>] | [host]]
列出所有端口。

logoff [-u <username>] message
注销用户。

ls
列出命令。

more [-p <page_size>]
进行分页。

pingdevice <[-id <device_id>] | [host]>
Ping 设备。

restartcc minutes [message]
重新启动 CC-SG。

restartdevice <[-id <device_id>] | [host]>
重启设备。

restoredevice <[-host <host>] | [-id <device_id>]> [backup_id]
恢复设备配置。

shutdowncc minutes [message]
关闭 CC-SG。

ssh [-e <escape_char>] <[-id <device_id>] | [host]>
打开到 SX 设备的 SSH 连接。

su [-u <user_name>]
更改用户。

upgradedevice <[-id <device_id>] | [host]>
升级设备固件。

exit
退出 SSH 会话。

键入命令后跟 **–h** 开关即可显示该命令的帮助，例如 **listfirmwares –h**。

命令提示

以下介绍 SSH 命令的几个细微差别：

- 对于传递 IP 地址的命令（例如 upgradedevice），可用主机名代替 IP 地址。对于主机名规则，参见**第 1 章：简介**中的“术语/缩略语”。
- copydevice 和 restartdevice 命令仅适用于部分 Raritan 设备（例如 Dominion SX）。这些命令不支持 IPMI 服务器和一般设备。

创建到 SX 设备的 SSH 连接

可创建到 SX 设备的 SSH 连接，从而在设备上执行管理操作。连接后，即可提供 SX 设备所支持的管理命令。

注：在连接之前，确保 SX 设备已经添加到 CC-SG。

1. 键入 **listdevices** 以保证 SX 已经添加到 CC-SG。

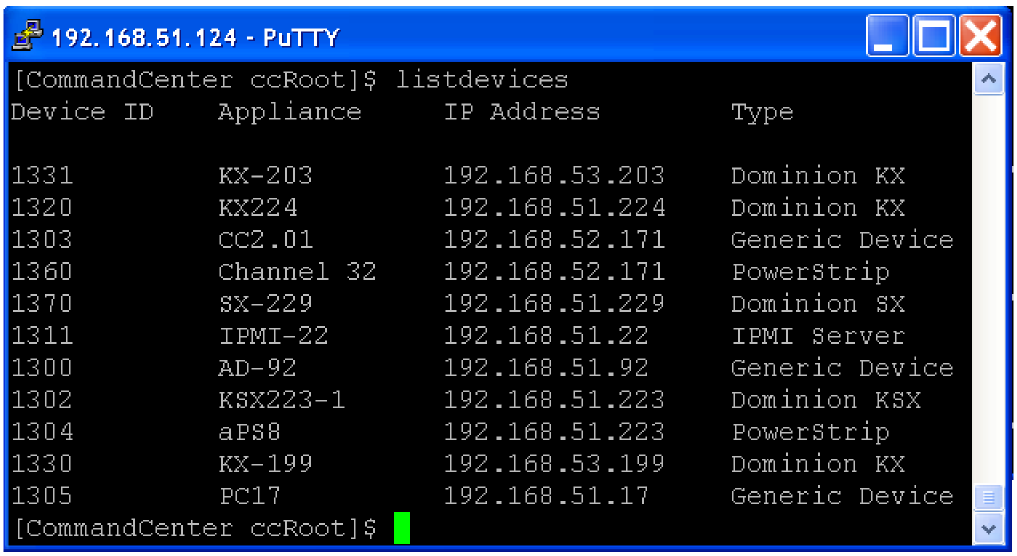


图 179 列出 CC-SG 上的设备

2. 键入 **ssh -id <device id>** 连接 SX 设备。例如使用上述屏幕，可键入 **ssh –id 1370** 连接到 SX-229。

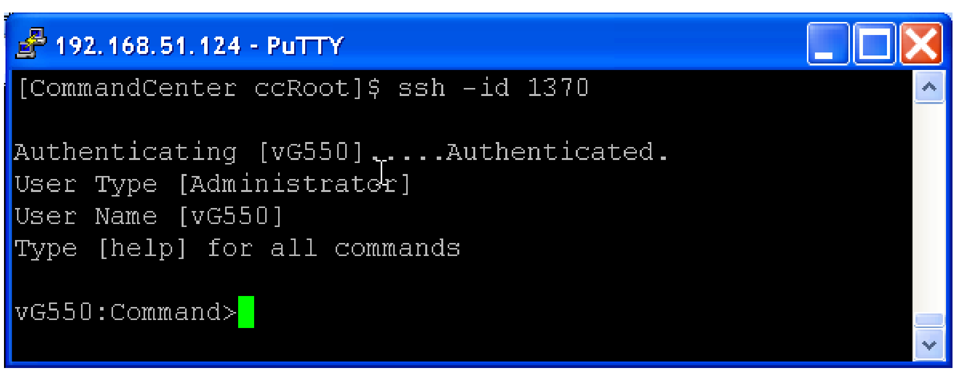


图 180 通过 SSH 连接 SX 设备

通过带外串口使用 SSH 连接节点

通过关联的带外串口可使用 SSH 连接节点。SSH 连接为代理模式。

1. 键入 **`listinterfaces`** 查看节点 ID 及其关联的接口。

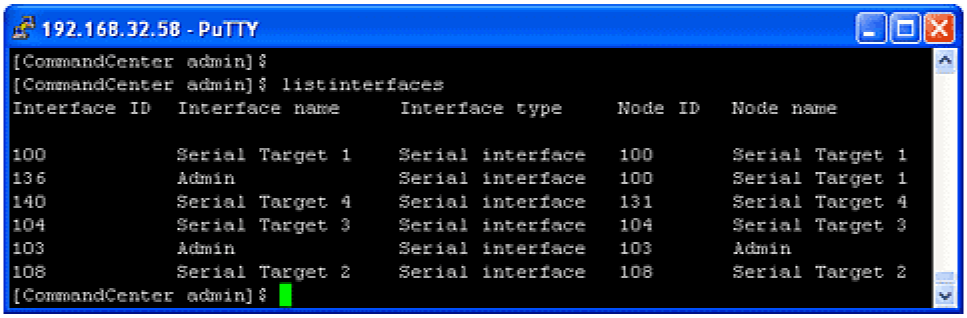


图 181 SSH 中的 Listinterfaces 命令

2. 键入 **`connect –i <interface_id>`** 连接与接口关联的节点。

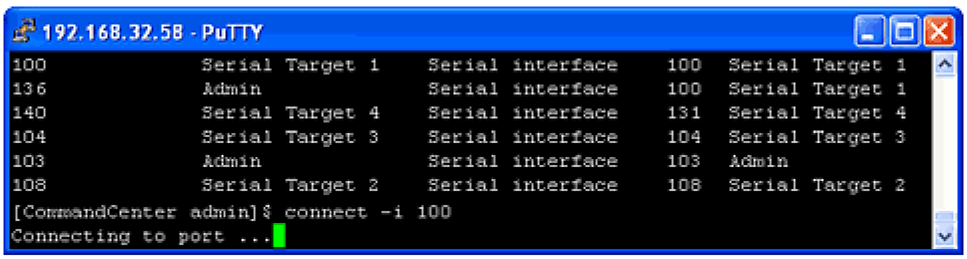


图 182 通过带外串口连接节点

3. 连接到节点后，键入默认的 Escape 键“~”后跟一个点“.”。在出现的提示符后面可输入特定的命令或别名，说明如下：

命令	别名	说明
quit	**q**	终止连接，返回 SSH 提示符。
get_write	**gw**	获取写访问权限。让 SSH 用户执行目标服务器的命令，而浏览器用户只能观察活动。
get_history	**gh**	获取历史。显示目标服务器上的上几条命令和结果。
send_break	**sb**	发送中断。中断由浏览器用户发起的目标服务器内的循环。
help	**?,h**	打印帮助屏幕。

退出会话

要退出到 CC-SG 的整个 SSH 连接，键入 **`exit`**。

诊断控制台

“诊断控制台”是提供到 CC-SG 本地访问的标准非图形界面。可通过串口或 KVM 端口访问，或通过 Secure Shell (SSH) 客户端（例如 Putty 或 OpenSSH 客户端）访问。

提供两个登录名：一个是 **status**，提供到状态控制台的访问；另一个是 **admin**，提供到管理员控制台的访问。所有登录用户名和密码均区分大小写。

关于状态控制台

在默认配置中，状态控制台不需要密码。在“登录”提示符后面键入 **status** 显示当前系统信息，这可用于确认 CC-SG、CC-SG 使用的各种服务以及所连网络的健康状态。

关于管理员控制台

管理员控制台的默认用户名/密码为 **admin/raritan**。admin 帐户允许设置一些初始参数、提供初始网络配置、调试日志文件，并执行一些有限的诊断和重新启动 CC-SG。诊断控制台的 **admin** 帐户是单独的，不同于 CC-SG 管理员的 Director Client 和基于 html 的 Access Client 所用的 **admin** 帐户和密码。两个用户可使用相同或者不同的密码。更改任一密码不会影响另一个。

注：如果通过 SSH 访问诊断控制台，则状态控制台和管理员控制台将继承在 SSH 客户端和键盘绑定中配置的外观设置，这可能与本文档的所有方面相符。

通过 VGA/键盘/鼠标端口访问诊断控制台

1. 将一台 VGA 监视器以及 PS2 键盘和鼠标连接到 CC-SG 设备的后部。
2. 视频监视器应检测到信号，在键盘上输入回车键应在屏幕上调出登录提示符：

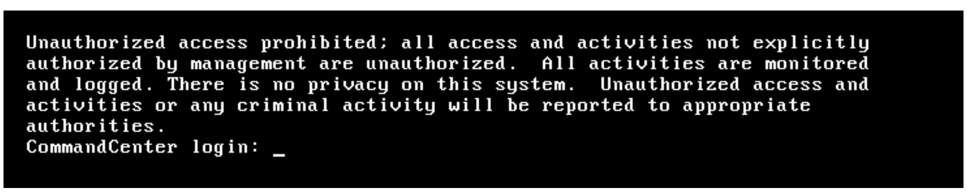


图 183 登录诊断控制台

通过 SSH 访问诊断控制台

1. 在与 CC-SG 有网络连接的客户端 PC 上，启动一个 SSH 客户端（例如 Putty）。
2. 指定 CC-SG 的 IP 地址或 IP 主机名（如果 CC-SG 与 DNS 服务器注册），并指定端口 23。
3. 单击允许进行连接的按钮。出现一个窗口，提示进行登录。

访问状态控制台

访问状态控制台不需要密码，但可以强制要求密码。

1. 在登录提示符后键入 **status**。显示只读的状态控制台。

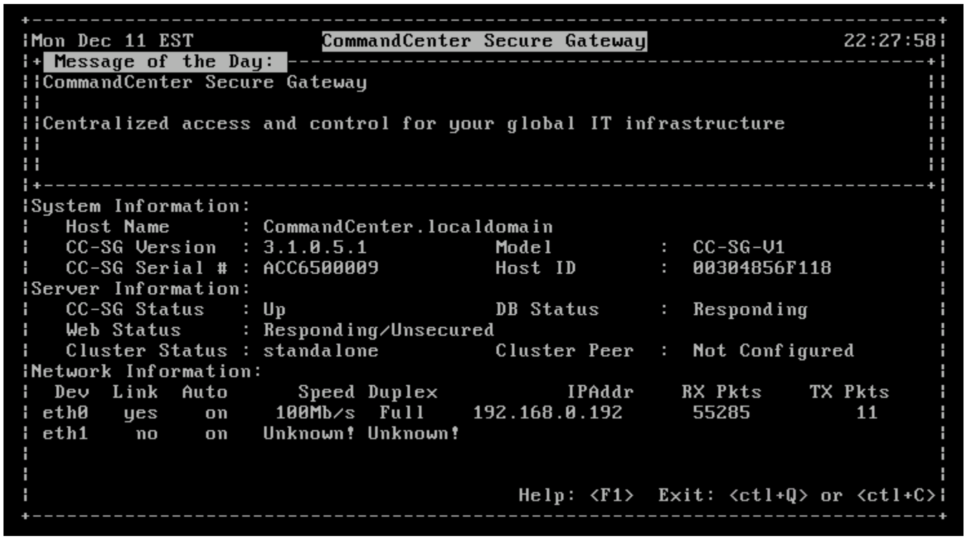


图 184 状态控制台

- 此屏幕动态显示系统的健康状况信息，以及 CC-SG 及其子组件是否工作。
- 屏幕右上角上的时间是 CC-SG 上最后一次轮询数据的时间。
- 此屏幕上的信息大约每 5 秒钟更新一次。
- 键入 **CTRL-L** 清除当前屏幕并重新载入更新的信息。最快可每秒更新屏幕一次。
- 按 **CTRL-Q** 或 **CTRL-C** 退出屏幕。
- 状态控制台不接受任何其它输入或屏幕导航。所有其它输入都将被忽略。

下表介绍 CC-SG 和 CC-SG 数据库的状态：

状态	说明
CC-SG 状态：运行	CC-SG 可用。
CC-SG 状态：停机	CC-SG 可能正在重新引导。如果继续处于该**停机**状态，请尝试重启 CC-SG。
CC-SG 状态：正在重启	CC-SG 正在重新启动。
DB 状态：正在响应	CC-SG 的数据库可用。
DB 状态：停机	CC-SG 可能正在重新引导。

访问管理员控制台

注：管理控制台上显示的所有信息都是静态的。如果通过 CC-SG GUI 或诊断控制台对配置进行了更改，则需要在配置生效后重新登录管理员控制台，才能在管理员控制台上看到变更。

1. 在登录提示符后键入 **admin**。
2. 键入 CC-SG 的“密码”。默认密码为 **raritan**。 首次登录时此密码会过期，必须选择新的密码。键入此密码，出现提示时再键入一个新密码。有关设置密码强度的详细信息，请参阅本章后面的“**诊断控制台密码 (Admin)**”部分。
3. 出现管理员控制台主屏幕。可执行初始系统网络接口配置、在“状态”窗口中编辑“当日消息”、查看日志文件。通过“文件”菜单可离开管理员控制台。

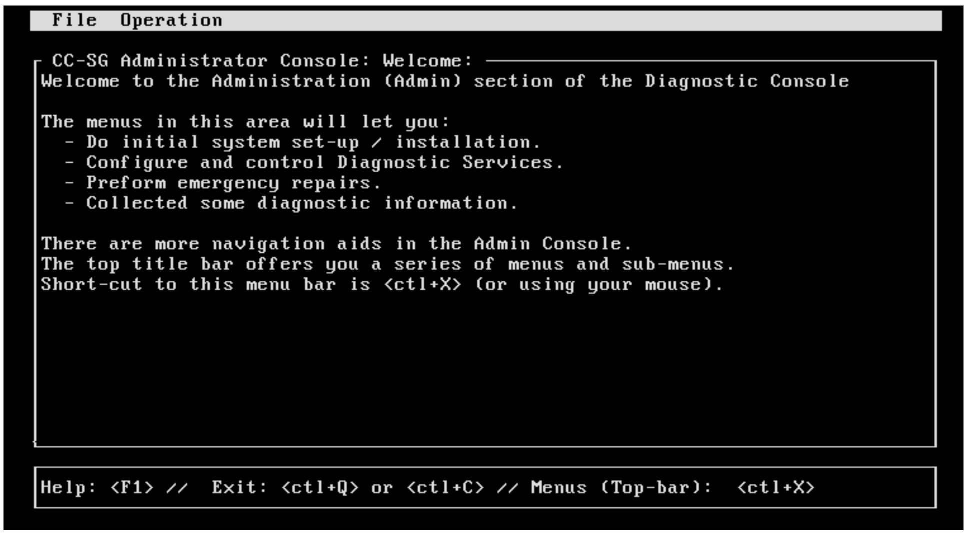


图 185 管理员控制台

导航管理员控制台

下表介绍在诊断控制台菜单中的各种导航方式。对于某些会话（尤其是 SSH），鼠标也可用于导航各种表格。但是，鼠标并非在所有 SSH 客户端或 KVM 控制台上都会有效。

按键	操作
CTRL+C 或 CTRL+Q	退出诊断控制台。
CTRL+L	清除屏幕并重绘信息（但信息本身并不被更新或刷新）。
TAB	移到下一个可用选项。
空格键	选择当前选项。
箭头键	允许移动到一个选项内的不同字段。
鼠标	允许指向和选择一个选项（如果可用）。

在诊断控制台中编辑有限服务协议和当日消息

在输入登录用户名之后输入密码之前，管理员控制台内会显示有限服务协议 (RSA) 消息。当日消息 (MOTD) 出现在状态控制台的顶部。

1. 要编辑 RSA（在诊断控制台中称为“登录前消息”）或 MOTD 消息，单击“操作”、“状态控制台配置”，然后单击“编辑登录前消息”或“编辑 MOTD”。
2. 使用 Delete 和 Backspace 键，在提供的框内键入新消息。对于 MOTD，最长可输入 76 个字符。

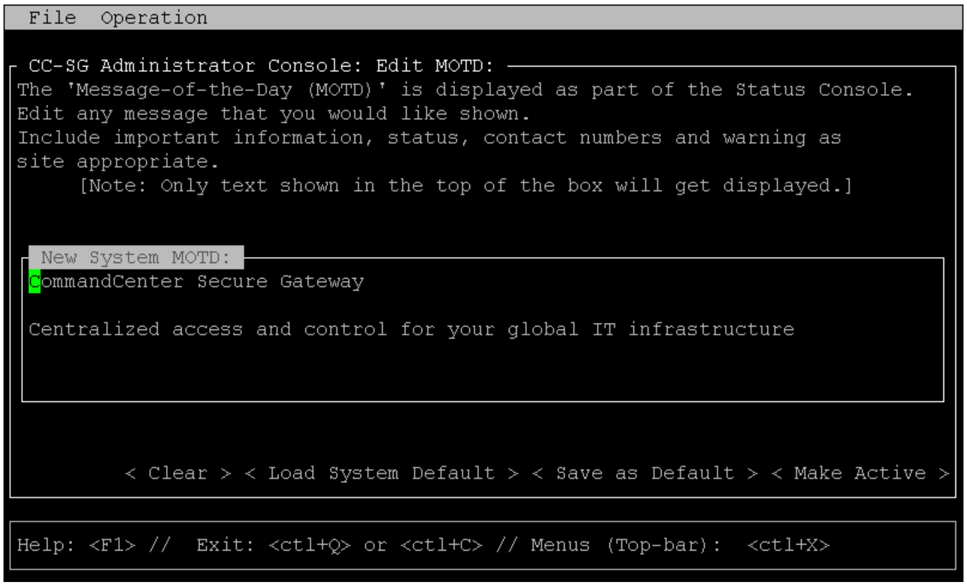


图 186 编辑状态控制台的 MOTD

3. 单击屏幕底部的“激活”，或按 Tab 键直到“激活”被选中，然后按一次空格键。
4. “登录前”和“当日消息”有三个不同的缓冲区或区域：

- 管理控制台屏幕——启动时使用“活动消息”缓冲区的副本，可被此用户/会话编辑。
- 保留原型或模型消息、并在不同系统复位之间保留的系统缓冲区
- 活动消息缓冲区（用户与系统交互时可以看到）。在系统重新启动或重新引导时也保持不变。

按钮	说明
清除	删除“管理员控制台”屏幕上当前显示的所有文本。对系统使用的值没有影响。
载入系统默认	将“管理员控制台”屏幕替换为“系统缓冲区”的内容。
保存为默认	将当前的“管理员控制台”屏幕放入“系统缓冲区”。对“活动消息”显示没有影响。
激活	将当前的“活动消息”替换为“管理员控制台”屏幕的内容。所有新用户将会看到新消息。

编辑诊断控制台配置

“诊断控制台”可通过串口或 VGA/键盘/鼠标 (KVM) 端口访问，或通过 Secure Shell (SSH) 客户端访问。对于每种端口类型，可配置是否允许 **status** 或 **admin** 登录、现场支持是否也可从端口访问诊断控制台。对于 SSH 客户端，也可配置应使用哪个端口号，只要没有其它 CC-SG 访问在使用所需的端口。

要编辑诊断控制台配置：

1. 单击“操作”、“诊断控制台配置”，然后单击“诊断控制台服务”。
2. 单击或使用 **Tab** 键、**↓↑** 键和**回车**键，确定要如何配置和访问诊断控制台。有三种诊断控制台访问机制：串口 (COM1)、KVM 控制台和 SSH（IP 网络）。诊断控制台提供三种服务：状态显示、管理控制台、Raritan 现场支持。此屏幕允许通过各种访问机制选择哪些服务可用。
3. 在“端口”字段中键入通过 SSH 访问诊断控制台的端口号。默认端口为 **23**。

重要说明：小心不要完全锁定所有管理或现场支持访问。

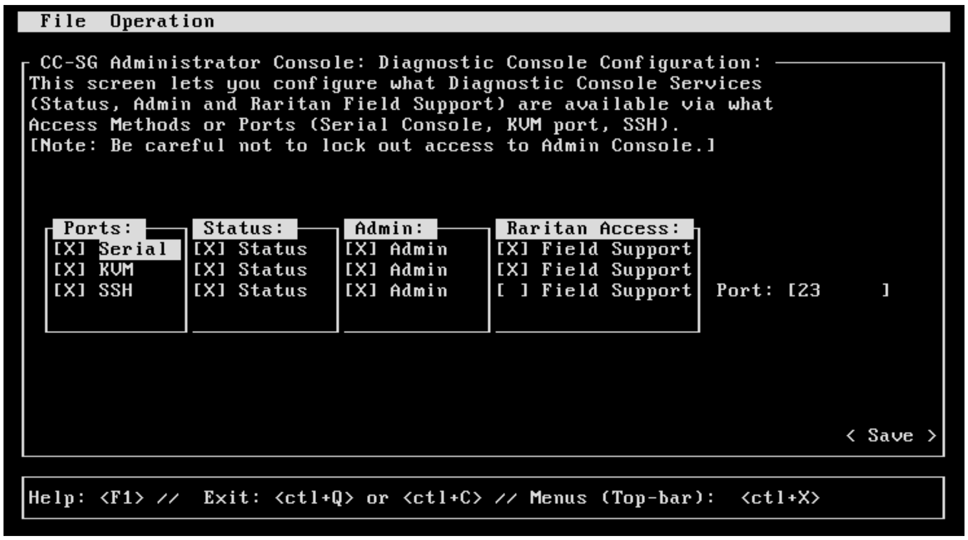


图 187 编辑诊断控制台配置

4. 单击屏幕底部的“保存”，或按 Tab 键直至“保存”被选中，然后按回车键。

编辑网络接口配置（网络接口）

在“网络接口”配置中，可执行初始设置任务，例如设置 CC-SG 的主机名和 IP 地址。用鼠标单击或者使用 Tab 和箭头键进行导航。按回车键选择值。

1. 要编辑网络接口配置，单击“操作”、“网络接口”，然后单击“网络接口配置”。
2. 如果网络接口已经配置，可看到一条“警告”消息，表示应使用 CC-SG GUI（管理员的 Director Client）配置接口。如果要继续，单击“是”。默认的“网络接口配置”屏幕如下所示：

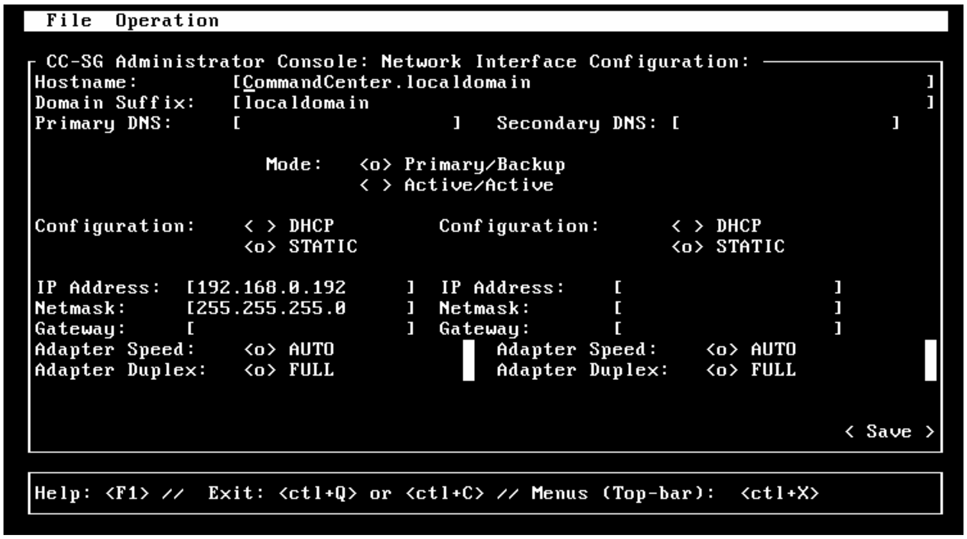


图 188 编辑网络接口

3. 在“主机名”字段内键入主机名。保存后，此字段将会更新，反映出完全限定的域名 (FQDN)（如果已知）。对于主机名规则，参见**第 1 章：简介**中的“**术语/缩略语**”。
4. 在“模式”字段中，选择“主/备份模式”或“活动/活动模式”。详情参阅本章前面的“**网络配置**”部分。按 Tab 键选择字段，然后按箭头键在两个模式之间选择。选择一种模式，然后按空格键。
5. 单击或用 Tab 键跳到“配置”字段，从列表中选择“DHCP”或“静态”。
   - 如果选择 DHCP 且 DHCP 服务器已经正确配置，则保存、退出并重新进入管理控制台后，后将自动填充 DNS 信息、域后缀、IP 地址、默认网关和子网掩码。
   - 如果选择“静态”，则键入“IP 地址”（必填）、“子网掩码”（必填）、“默认网关”（可选）、“主用 DNS”（可选）和“备用 DNS”（可选）信息，并在“域后缀”（可选）中键入域名。
   - 即使在使用 DHCP 来确定接口的 IP 配置，仍要提供正确格式的 **IP 地址**和**子网掩码**。用 Tab 键跳到“适配器速度”并使用 ↓↑ 键从列表中选择一个线速。其它值

   10、100 和 1000 Mbps 在一个可滚动的列表（其中任何时候只能看到一个值）内，↓↑ 键用于在他们之间导航，空格键用户选择一个替代值（如果需要）。

7. 如果对于“适配器速度”没有选择“自动”，单击“适配器双工”并使用 ↓↑ 键从列表中选择一个双工模式（“全双工”或“半双工”）（如果适用）。虽然在任何时候只能选择一种双工模式，但只有“适配器速度”不是“自动”时才有意义并且生效。
8. 如果选择“活动/活动模式”，重复这些步骤配置第二个网络接口。
9. 选择“保存”保存更改。CC-SG 将重新启动，注销所有 CC-SG GUI 用户，并终止其会话。将出现一个“警告”屏幕，通知即将进行网络重新配置以及相关的 CC-SG GUI 用户影响。选择“是”继续进行。

10. 在诊断控制台的状态屏幕内可监视系统进度。在 KVM 端口上，键入 <**ALT**>+<**F2**> 并用 status 登录，可选择另一个终端会话。键入 <**ALT**>+<**F1**> 可返回到原来的终端会话。在 <**F1**> 至 <**F6**> 上有六个可用的终端会话。对于 SSH 访问，从客户端启动另一个 SSH 会话并用 **status** 登录应该能够成功，只要网络重新配置允许连接。

Ping IP 地址（网络接口）

Ping 用于检测 CC-SG 计算机与特殊 IP 地址之间的连接是否正常。

注：有些站点明确阻止 ping 请求。请验证目标和中间网络允许 ping 操作，然后才能判断是否存在问题。

1. 单击“操作”，“网络接口”，然后单击“Ping”。
2. 在“Ping 目标”字段中输入要检查目标的 IP 地址或主机名（如果在 CC-SG 上正确配置 DNS）。
3. 以下选项为可选内容：

选项	说明
显示收到的其它 ICMP 包	详细输出，除了 ECHO_RESPONSE 包以外还列出其它收到的 ICMP 包。很少看到。
无 DNS 解析	不解析地址或主机名。
记录路由	记录路由。设置 IP 记录路由选项，将在 IP 标头内存储包的路由。
使用广播地址	允许 Ping 广播消息。
自适应同步	自适应 Ping。包之间的时间间隔调整为往返时间，使网络中不会超过一个无反应的探测。最小时间间隔为 200 毫秒。

4. 或者，键入执行 Ping 命令的时间（秒）、发送的 Ping 请求个数、Ping 包的大小（默认值为 56，与 8 字节的 ICMP 标头数据合并时将转换为 64 个 ICMP 数据字节）。如果留空，则使用默认值。
5. 单击窗口右下角的“Ping”。如果结果显示一些列的应答，则连接正常。时间反映出连接的快慢。如果看到“超时”错误而非应答，则计算机与域之间存在中断。在这种情况下，要执行一次跟踪路由——参见下节。
6. 按 **CTRL+C** 键终止 Ping 会话。系统出现提示符“Return?”，然后返回到诊断控制台（这样可根据需要查看和分析任何输出）。

*注：按 **CTRL+Q** 键显示迄今为止会话的统计摘要，并继续 Ping 目标。*

使用跟踪路由（网络接口）

跟踪路由通常用于网络故障排除。通过显示遍历的路由器列表，允许您识别从您的计算机到网络上特殊目标所采用的路径。它将列出所通过的路由器，一直到达目标或者失败和放弃。除此以外，它还告诉您路由器之间每一“跳”的长度。这可以帮助识别路由问题或阻止到某个站点访问的防火墙。

要在 IP 地址或主机名上执行跟踪路由：

1. 单击“操作”，“网络接口”，然后单击“跟踪路由”。
2. 在“跟踪路由目标”字段中输入要检查目标的 IP 地址或主机名。
3. 以下选项为可选内容：

选项	说明
详细	详细输出，除了 TIME_EXCEEDED 和 UNREACHABLE 以外还列出其它收到的 ICMP 包。
无 DNS 解析	不解析地址或主机名。
使用 ICMP （相对于正常 UDP）	使用 ICMP ECHO 代替 UDP 数据报。

4. 可选地键入跟踪路由命令在出站探测包中将使用多少跳（默认为 30）、探测中要使用的 UDP 目标端口（默认为 33434）以及跟踪路由包的大小。如果留空，则使用默认值。
5. 单击窗口右下角的“跟踪路由”。
6. 按 **CTRL+C** 或 **CTRL+Q** 键终止跟踪路由会话。出现 **Return?** 提示符，按回车返回跟踪路由菜单。因为发生“目标已达”或“超过跳次数”事件而终止跟踪路由时，也会出现 **Return?** 提示符。

编辑静态路由（网络接口）

在“静态路由”中，可查看当前 IP 路由表，修改、添加和删除路由。小心使用和替换静态路由可有效地改善网络性能，允许为重要的业务应用程序保留带宽，在每个接口附加在单独的 IP 域的“活动/活动”网络设置中会非常有用——详见第 12 章：高级管理中的“网络配置”。用鼠标单击或使用 **Tab**、↓↑键导航，或按**回车**键选择值。

要查看或更改静态路由：

1. 单击“操作”，“网络接口”，然后单击“静态路由”。
2. 显示当前的 IP 路由表。可添加主机或网络路由，或删除路由。“刷新”按钮可更新上表内的路由信息。

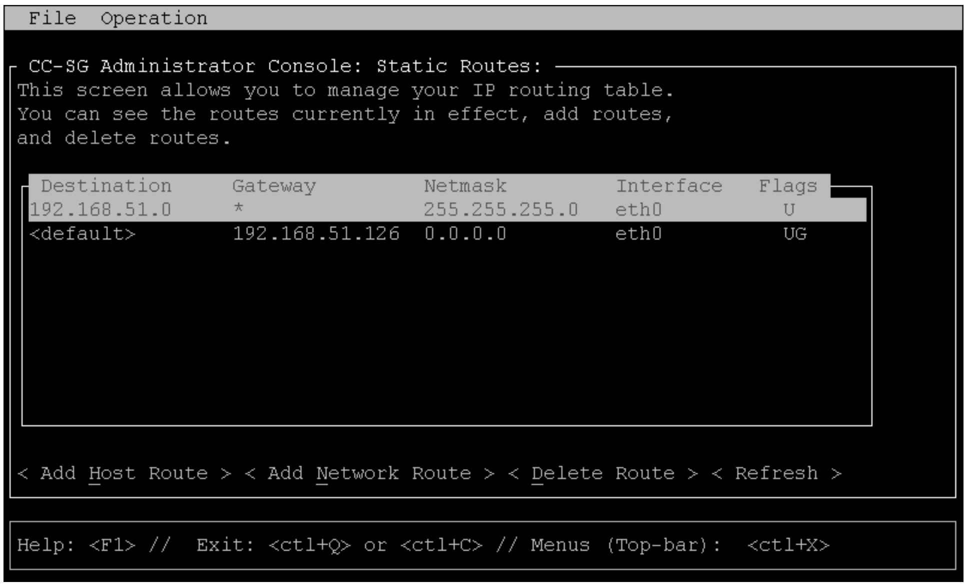


图 189 编辑静态路由

查看日志文件 (Admin)

可通过 LogViewer 同时查看一个或多个日志文件，这样可一次浏览多个文件来检查系统活动。

要查看日志文件：

1. 单击“操作”、“管理”，然后单击“系统日志文件查看器”。
2. Logviewer 屏幕分成四个主区域（参见下面的屏幕）：
   - 系统中当前可用的“日志文件列表”。如果列表比显示窗口长，则可用箭头键滚动列表。
   - “日志文件列表”排序标准。日志文件可按照完整文件名称、最近更改的日志文件或最大文件大小进行排序。
   - 查看器显示选项（详见下文）。
   - 导出/查看选择器。

3. 用鼠标单击或使用箭头键导航，按**空格键**选择一个日志文件用 **X** 标记。可同时查看多个日志文件。

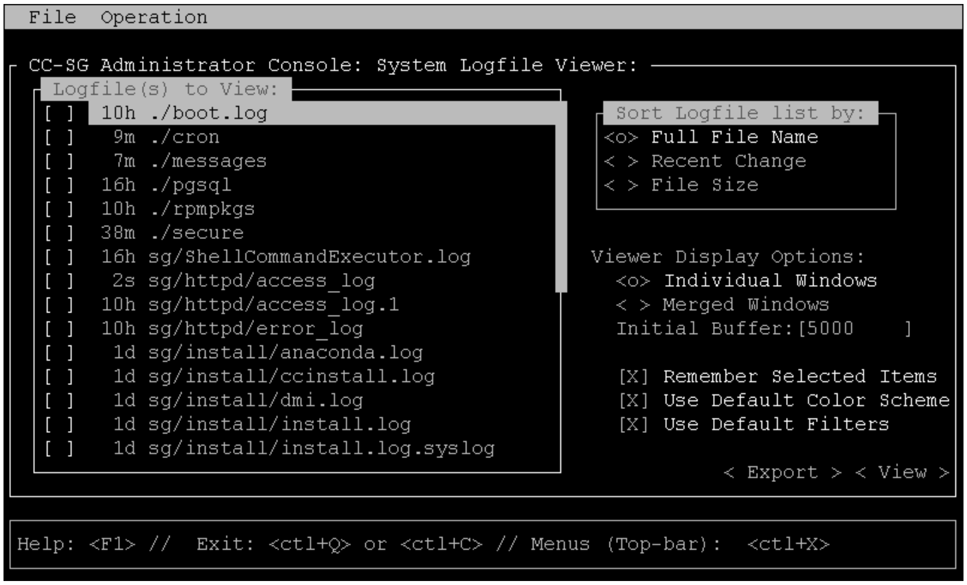


图 190 选择要查看的日志文件

只有关联的列表变为活动（如用户进入日志文件列表区域）或者选择新的排序选项时，“日志文件”列表才会更新。文件名前面带有一个时间戳，表示日志文件最近何时收到新数据，或者带有日志文件的文件大小。时间戳为 s → 秒、m → 分、h → 时和 d → 天。文件大小为 B → 字节、K → 千 (1000) 字节、M → 兆 (1,000,000) 字节和 G→ 吉字节。当排序选项为“完整名称”或“最近更改”时，将会使用时间戳，而文件大小则用于“文件大小”。

“日志文件列表排序标准”窗口包含一些单选按钮（互斥），控制这“要查看的日志文件”窗口中日志文件显示的顺序。

选项	说明
单独窗口	在单独的子窗口中显示所选的日志。
合并窗口	将所选日志合并到一个显示窗口。
初始缓冲区	设置初始缓冲区或历史大小。默认值为 **5000**。系统被配置为缓冲所有出现的新信息。
记住选定项目	如果此框选中，则会记住当前的日志文件选择（如果有）。否则，每次生成新的日志文件列表时，选择将被复位。如果要逐个操作文件，这个选择会非常有用。
使用默认颜色方案	如果此框选中，部分日志文件将使用标准的颜色方案查看。注：在查看日志文件时，可用多个命令来更改颜色方案。
使用默认过滤器	如果此框选中，部分日志文件将应用自动过滤器。
导出	此选项包装所有选择的日志文件并通过 Web 访问提供，使其能被 Raritan 技术支持检索或转发给 Raritan 技术支持。客户不能访问访问此包的内容。导出的日志文件将提供最长 10 天，然后系统将自动将其删除。
查看	查看所选日志。

当选择“查看”以及“单独窗口”时，显示 LogViewer：

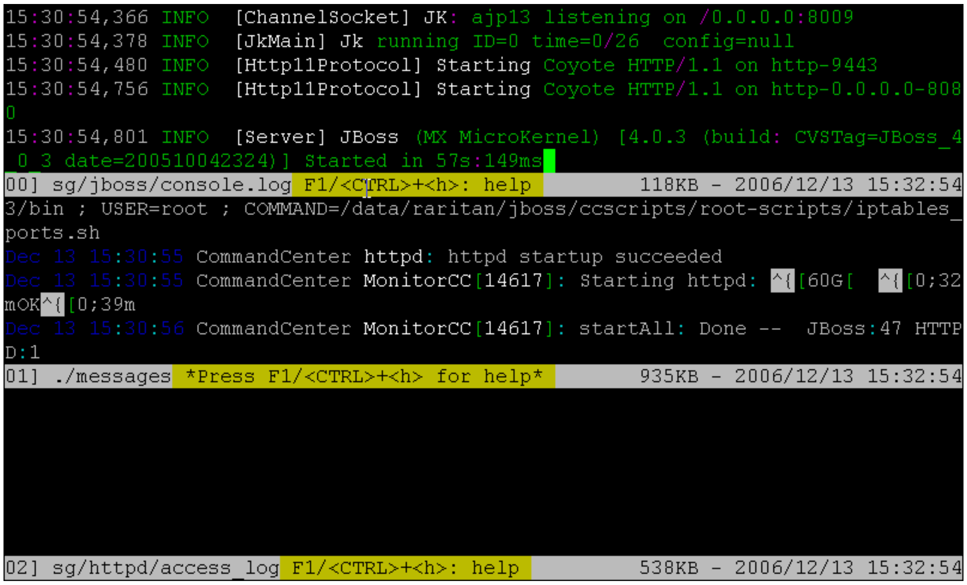


图 191 选择要查看的日志文件

4. 查看日志文件时，键入 **q**、**CTRL-Q** 或 **CTRL+C** 返回到上一屏幕。
5. 如果需要，可更改日志文件中的颜色以突出显示重要部分。键入 c 可更改日志文件的颜色，并且如果选择查看多个日志文件，将从列表中选择一个日志。

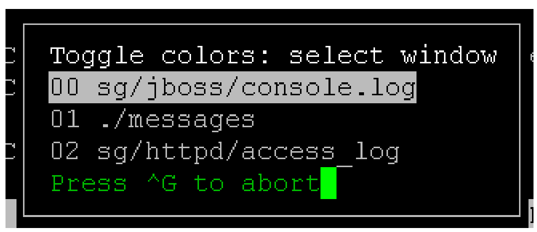


图 192 更改日志文件的颜色

6. 键入 **i** 显示系统信息。

注：到此管理员控制台会话启动之时，系统载荷是静态的——使用 TOP 实用工具可动态地监视系统资源。

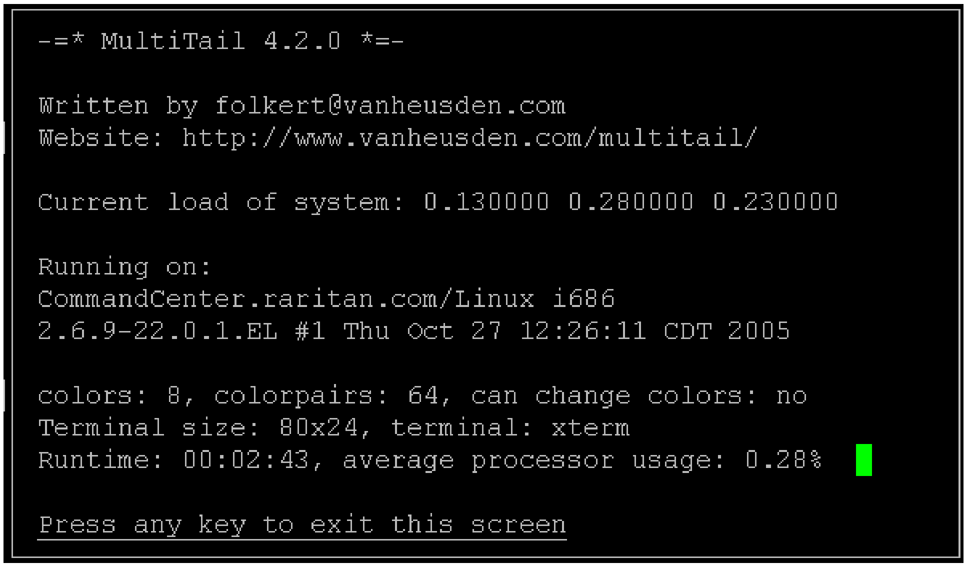


图 193 显示信息

7. 如果需要，可使用常规表达式过滤日志文件。键入 **e** 可添加或编辑常规表达式，并且如果选择查看多个日志文件，将从列表中选择一个日志。

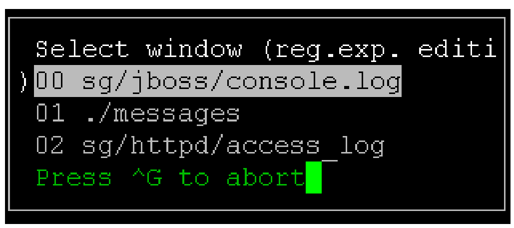


图 194 在日志文件中添加表达式

8. 键入 **a** 添加一个常规表达式。例如，如果想要显示 **sg/jboss/console.log** 日志文件中 **WARN** 消息上的信息，输入 **WARN** 并选择 **match**。

注：此屏幕还显示 console.log 的“默认过滤器方案”，这会删除大部分的 Java 堆消息。



图 195 为日志文件指定常规表达式

9. 选择 **F1** 可获得所有 LogViewer 选项的帮助。按 **CTRL+C** 和 **CTRL+Q** 可终止此 LogViewer 会话。

重新启动 CC-SG (Admin)

可重新启动 CC-SG，这将注销所有当前的 CC-SG 用户，并终止他们到远程目标服务器的会话。

重要说明：强烈建议在 CC-SG GUI 中重新启动 CC-SG，除非绝对需要在此进行重新启动。详情参阅第 11 章：系统维护中的“重新启动 CC-SG”。在诊断控制台中重新启动 CC-SG 不会将正在重新启动的消息通知 CC-SG GUI 用户。

要重新启动 CC-SG：

1. 单击“操作”、“管理”，然后单击“CC-SG 重新启动”。
2. 单击“重新启动 CC-SG 应用程序”，或者按回车键。在下一个屏幕中确认重新启动继续。

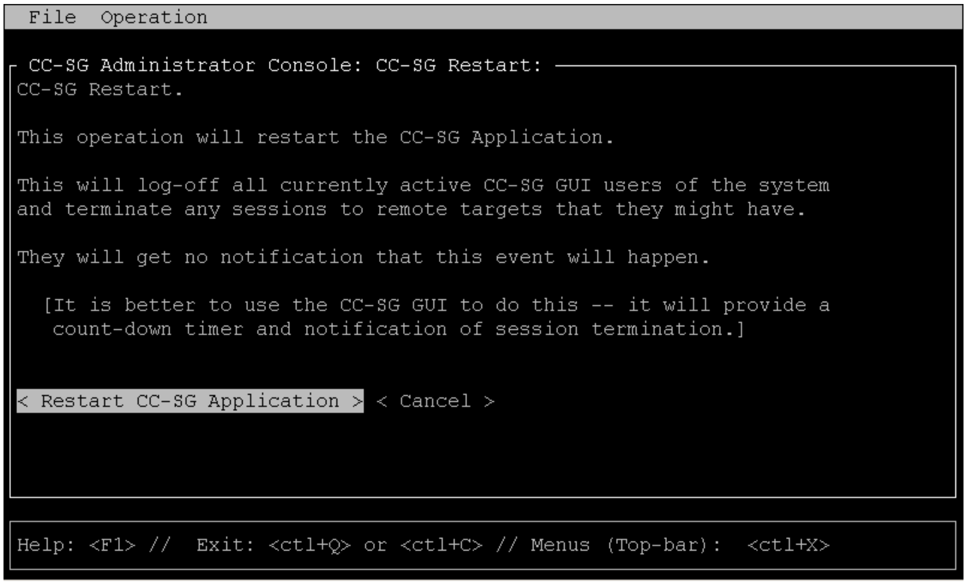


图 196 在诊断控制台中重新启动 CC-SG

重新引导 CC-SG (Admin)

此选项将重新引导整个 CC-SG，模拟一次电源循环。用户将不会收到通知。CC-SG、SSH 以及诊断控制台用户（包括此会话）都将被注销。所有到远程目标服务器的连接也被终止。

要重新引导 CC-SG：

1. 单击“操作”、“管理”，然后单击“CC-SG 系统重新引导”。
2. 单击“重新引导系统”或按回车键即重新引导 CC-SG。在下一个屏幕中确认重新引导继续。

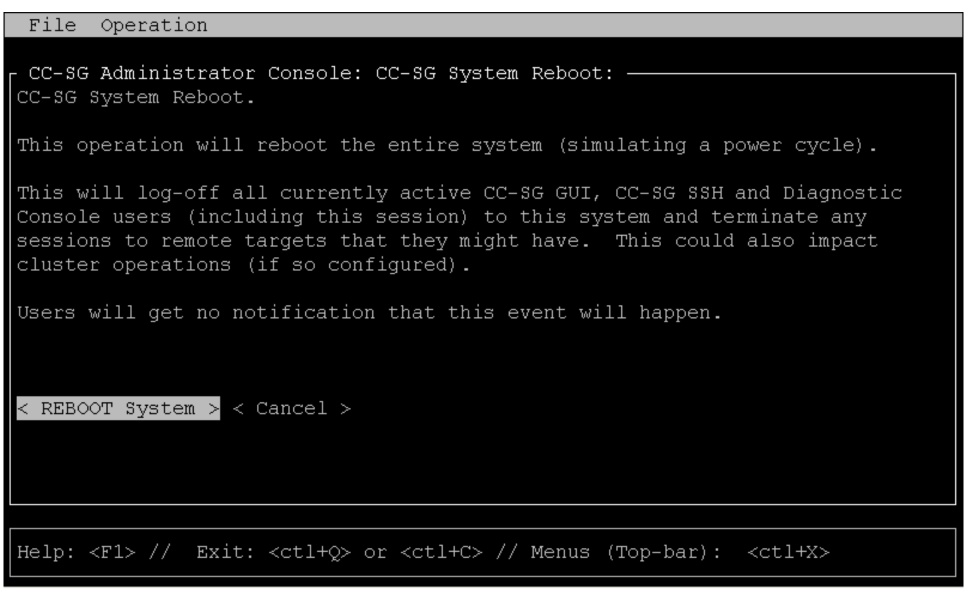


图 197 在诊断控制台中重新引导 CC-SG

关闭 CC-SG 系统 (Admin)

此选项将关闭整个 CC-SG。用户将不会收到通知。CC-SG、SSH 以及诊断控制台用户（包括此会话）都将被注销。所有到远程目标服务器的连接也被终止。防止将 CC-SG 重新开机的唯一方法就是按下设备前面的电源按钮。

要关闭 CC-SG：

1. 单击“操作”、“管理”，然后单击“CC-SG 系统关机”。
2. 单击“关闭 CC-SG”或者按回车键即去除 CC-SG 的交流电源。在下一个屏幕中确认关机操作继续。

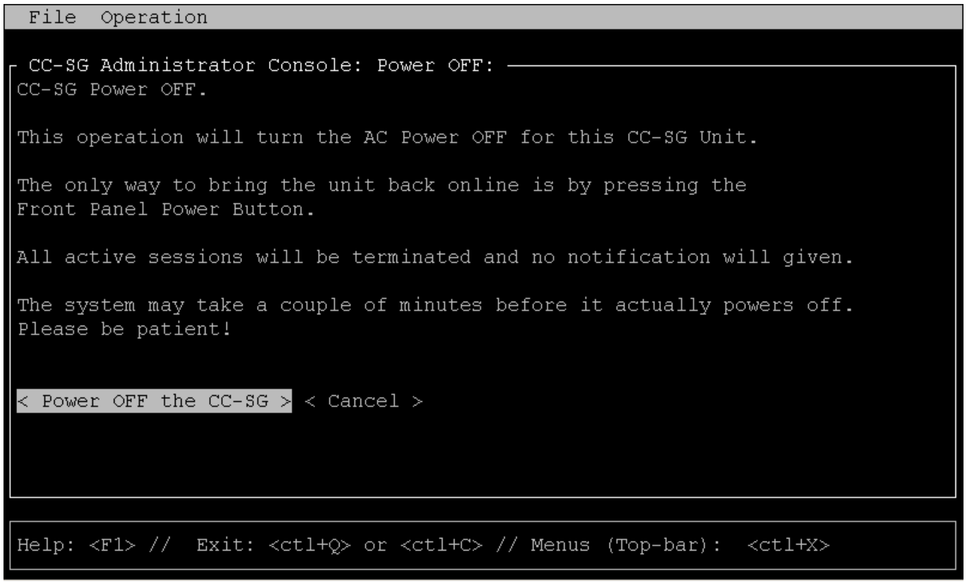


图 198 在诊断控制台中关闭 CC-SG

复位 CC-SG (GUI) 管理员密码 (Admin)

此选项将管理帐户 CC-SG GUI 用户的密码复位到所记录的出厂默认值。

注：这不是诊断控制台管理用户的密码。有关更改此帐户密码的详细信息，请参阅下面的“DiagCon 密码”部分。

要复位 CC-SG GUI 管理员密码：

1. 单击“操作”、“管理”，然后单击“CC-SG 管理密码复位”。
2. 单击“复位 CC-SG 管理密码”或按回车键，即将管理密码更改会出厂默认值。在下一个屏幕中确认密码复位继续。

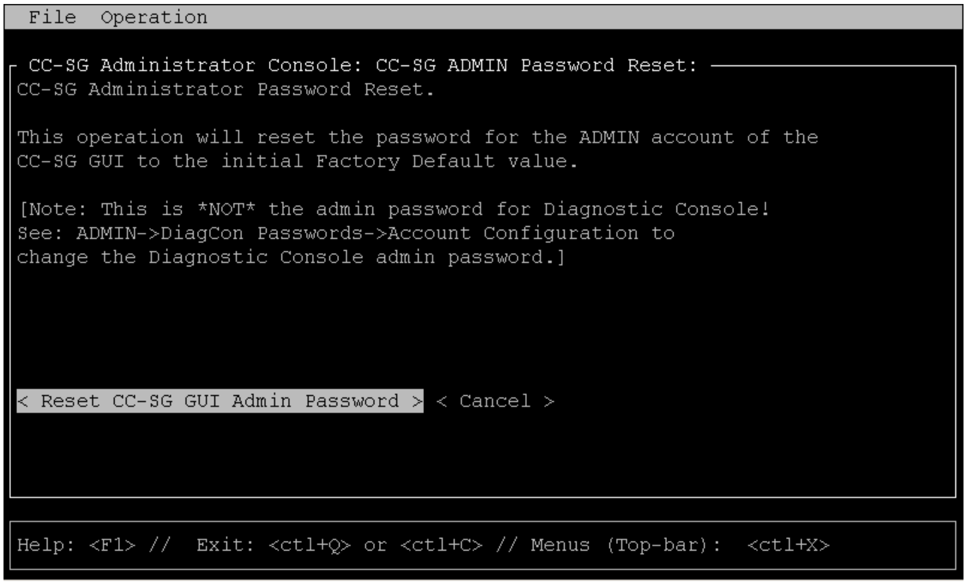


图 199 在诊断控制台中复位 CC-SG 的管理密码

复位 CC-SG 出厂配置 (Admin)

此选项将 CC-SG 系统的所有和部分都复位到出厂默认值。所有活动的 CC-SG 用户将被注销且不通知，SNMP 处理将会停止。强烈建议先将 CC-SG 置于维护模式，然后再开始此操作。如果可能，在管理员的 Director Client 中复位 CC-SG，而不是从诊断控制台进行复位。“Director Client 复位”选项可执行此处列出的所有功能，但复位网络值除外。

1. 在“操作”菜单中，单击“管理”，然后单击“出厂复位”。出现下面的屏幕，带有七个“复位选项”。

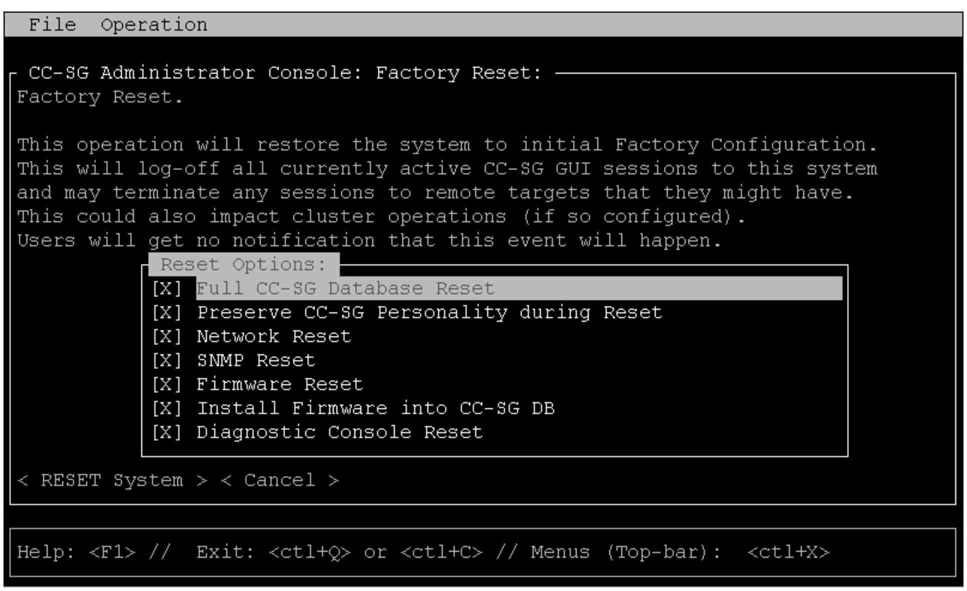


图 200 复位 CC-SG 出厂配置

选项	说明
完整 CC-SG 数据库复位	选择此选项将完全删除现有的 CC-SG 数据库，从头开始建立一个新的版本并加载所有出厂默认值。
复位时保留 CC-SG 个性	只有同时选择前一个选项时，此选项才会有效可用。由于 CC-SG 数据库正被重建（在前一个选项中），下面的值将被移植到新版本的数据库中（如果这些数据可读并可用；否则将使用默认值）。并尝试保留下列信息。默认值为括号中的内容。 • PC 客户端和 CC-SG 之间的安全通信（不安全） • 严格密码复选框选择是否启用严格密码强制（关） • 直接或代理连接（直接）选择 PC 客户端到带外节点使用直接或代理连接。 • 休止状态定时器（1800），注销空闲会话前的时间 • 调制解调器设置（10.0.0.1/10.0.0.2/<none>），调制解调器的服务器 IP 地址、客户端 IP 地址和回拨电话号码设置。
网络复位	此选项将网络置为出厂默认值： • 主机名称 = CommandCenter • 域名 = localdomain • 模式 =主/备份 • 配置 = 静态 • IP 地址 = 192.168.0.192 • 网络掩码 = 255.255.255.0 • 网关 = <无> • 主用 DNS = <无> • 备用 DNS = <无> • 适配器速度 = 自动
SNMP 复位	将 SNMP 配置复位到出厂默认值： • 端口：161 • 只读公用串：public • 读写公用串：private • 系统联系人、名称、位置：<空> • SNMP 陷阱配置 • SNMP 陷阱目标
固件复位	删除上载的固件文件，将默认版本恢复到文件系统存储库，但对 CC-SG DB 不做任何更改。
将固件安装到 CC-SG DB	将在基于文件系统的存储库中找到的固件文件载入 CC-SG DB。
诊断控制台复位	将诊断控制台恢复到原始出厂配置、帐户设置和默认值。

诊断控制台密码 (Admin)

此选项允许配置密码强度（status 和 admin），并允许配置密码属性，例如设置密码必须更改之间最大持续天数（应通过“帐户配置”菜单完成）。这些菜单中的操作仅适用于诊断控制台帐户（status 和 admin）和密码，对常规的 CC-SG GUI 帐户和密码没有影响。

密码配置

1. 单击“操作”、“管理”，“DiagCon 密码”，然后单击“密码配置”。
2. 在“密码历史深度”字段中，键入将被记住的密码个数。默认设置为 **5**。

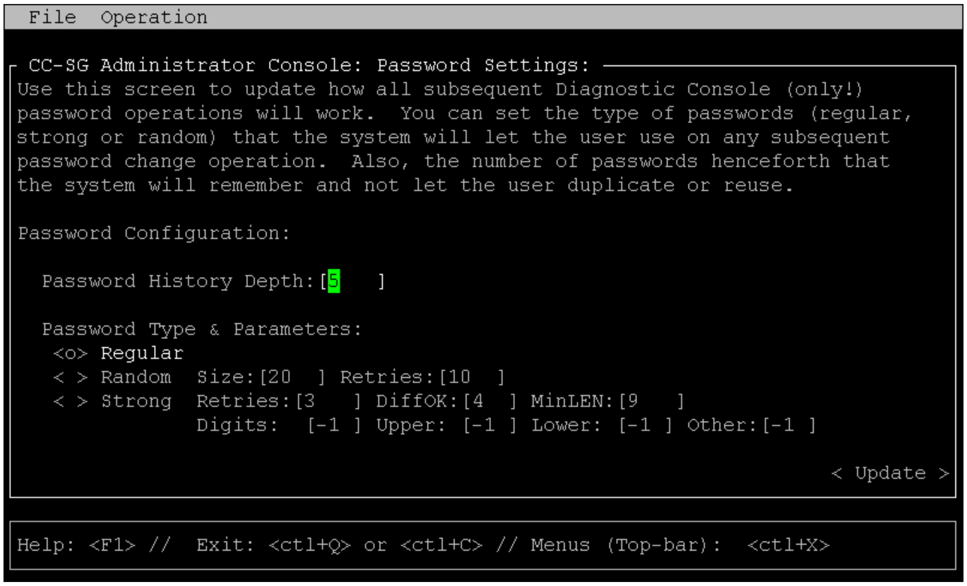


图 201 配置密码设置

3. 为 admin 和 status（如果启用）密码选择“正常”、“随机”或“严格”。

密码设置	说明
正常	这是标准选择。密码应大于 4 个字符，极少存在限制。这是系统默认的密码配置。
随机	提供随机生成的密码。配置最大密码大小（单位为位，最小是 14，最大是 70，默认是 20）、重试次数（默认为 10），这是询问是否接受新密码的次数。可接受（通过键入两次新密码）或拒绝随机密码。不能选择自己的密码。
严格	强制严格密码。“重试次数”为出现错误消息时提示的次数。**DiffOK** 表示新密码现对于老密码可有多少个相同的字符。**MinLEN** 是密码要求的最小长度。指定密码中需要多少位、大写字母、小写字母和其它（特殊）字符。正数表示向“简单”计数可累计此字符类的最大“信用”数量。负数表示密码必须至少要有那么多给定类别的字符。因此，数字“-1”表示每个密码中必须至少一个该类别的字符。

帐户配置

默认情况下，**status** 帐户不需要密码，但可在此处配置一个密码。可配置 **admin** 密码的其它方面，可启用或禁用现场支持帐户。

1. 要配置帐户，单击“操作”、“管理员”、“DiagCon 密码”，然后单击“帐户配置”。
2. 在出现的屏幕内，可查看每个帐户的设置，即 **Status**、**Admin**、**FS1** 和 **FS2**。

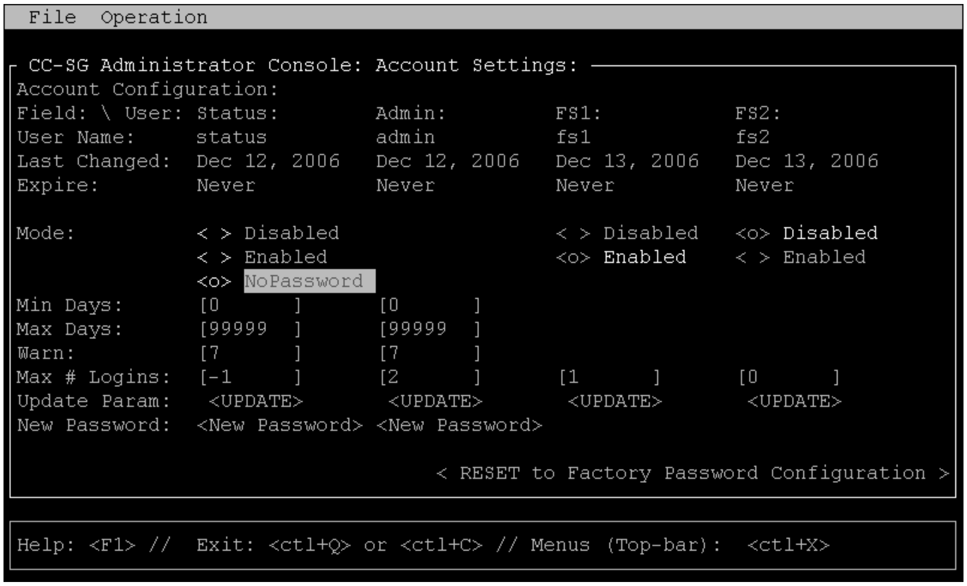


图 202 配置帐户

此屏幕划分成三个主要区域：

- 顶部显示系统帐户相关的只读信息。
- 中部显示每个 ID 相关的各种参数，还有几个按钮可允许更新这些参数或为帐户提供新密码。
- 最后的区域将密码配置恢复为出厂默认（或者系统最初交付时的状态）。

3. 如果需要为 **status** 帐户配置密码，请选择它下面的“已启用”。
4. 对于 **Admin** 和 **Status** 帐户，可配置以下内容：

设置	说明
用户/用户名	（只读）。这是此帐户的当前用户名或 ID。
上次更改日期	（只读）。这是此帐户上次密码更改的日期。
期满	（只读）。此帐户必须更改密码的日期。
模式	可配置选项：帐户是否被禁用（不允许登录）或启用（需要认证令牌）、或允许访问且不需要密码。（不要同时锁定 Admin 和 FS1 帐户，否则将无法使用诊断控制台。）
最小天数	密码更改后可再次更改的最小天数。默认值为 **0**。
最大天数	密码保持有效的最大天数。默认值为 **99999**。
警告	密码过期之前发出警告消息的天数。
最大登录个数	帐户允许的最大同时登录个数。负数表示没有限制（status 登录的默认值为 **-1**）。**0** 表示无人可以登录。正数定义可同时登录的用户个数（admin 登录的默认值为 **2**）。

更新	保存为此 ID 所做的任何更改。
新密码	输入帐户的新密码。

显示磁盘状态（实用工具）

此选项显示 CC-SG 磁盘的状态，例如磁盘大小、是否活动和运行、RAID-1 的状态、各种文件系统当前所用的空间大小。

要显示 CC-SG 的磁盘状态：

1. 单击“操作”、“实用工具”，然后单击“磁盘状态”。
2. 单击“刷新”或按**回车**键刷新显示。在升级或安装时刷新显示会非常有用，在 RAID 磁盘重建时和同步时可以看到进度。

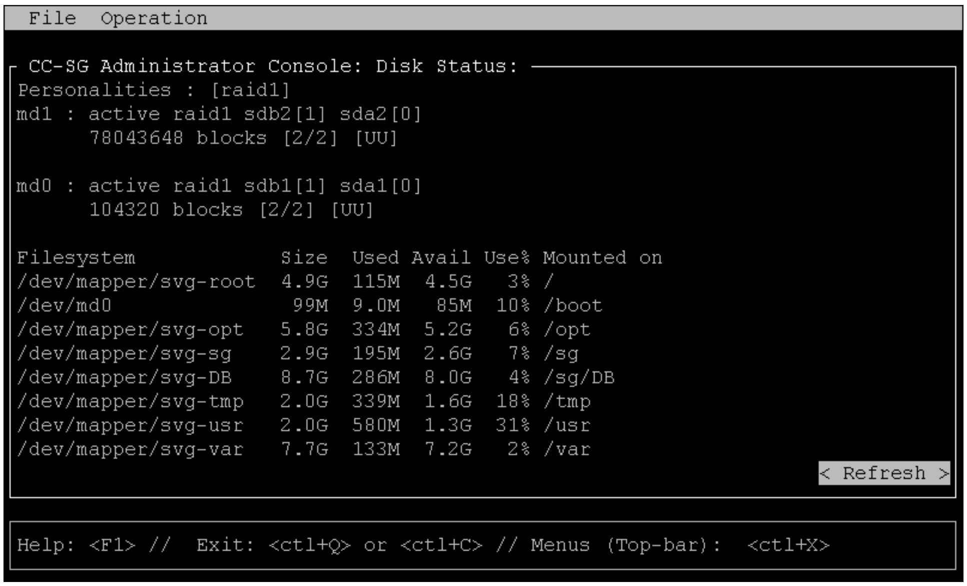


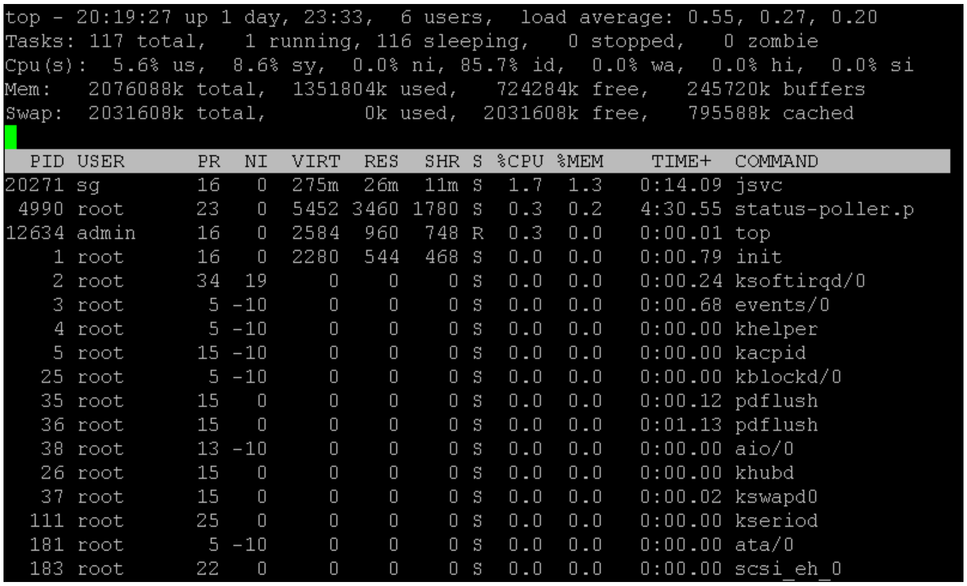
图 203 在诊断控制台中显示 CC-SG 的磁盘状态

***注：**当看到上述屏幕时，磁盘驱动器完全同步并提供完全 RAID-1 保护。**md0** 和 **md1** 阵列的状态都是 **[UU]**。*

显示 Top 显示（实用工具）

此选项显示 CC-SG 上当前运行的进程列表及其属性，以及整体的系统健康状态。

1. 要显示 CC-SG 上运行的进程，单击“操作”、“实用工具”，然后单击“Top 显示”。
2. 查看全部正在运行的、休眠的以及停止的进程总数。



```
top - 20:19:27 up 1 day, 23:33,  6 users,  load average: 0.55, 0.27, 0.20
Tasks: 117 total,   1 running, 116 sleeping,   0 stopped,   0 zombie
Cpu(s):  5.6% us,  8.6% sy,  0.0% ni, 85.7% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:   2076088k total,  1351804k used,   724284k free,   245720k buffers
Swap:  2031608k total,        0k used,  2031608k free,   795588k cached

  PID USER       PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
20271 sg         16   0  275m  26m  11m S  1.7  1.3   0:14.09 jsvc
 4990 root       23   0  5452 3460 1780 S  0.3  0.2   4:30.55 status-poller.p
12634 admin      16   0  2584  960  748 R  0.3  0.0   0:00.01 top
    1 root       16   0  2280  544  468 S  0.0  0.0   0:00.79 init
    2 root       34  19     0    0    0 S  0.0  0.0   0:00.24 ksoftirqd/0
    3 root        5 -10     0    0    0 S  0.0  0.0   0:00.68 events/0
    4 root        5 -10     0    0    0 S  0.0  0.0   0:00.00 khelper
    5 root       15 -10     0    0    0 S  0.0  0.0   0:00.00 kacpid
   25 root        5 -10     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
   35 root       15   0     0    0    0 S  0.0  0.0   0:00.12 pdflush
   36 root       15   0     0    0    0 S  0.0  0.0   0:01.13 pdflush
   38 root       13 -10     0    0    0 S  0.0  0.0   0:00.00 aio/0
   26 root       15   0     0    0    0 S  0.0  0.0   0:00.00 khubd
   37 root       15   0     0    0    0 S  0.0  0.0   0:00.02 kswapd0
  111 root       25   0     0    0    0 S  0.0  0.0   0:00.00 kseriod
  181 root        5 -10     0    0    0 S  0.0  0.0   0:00.00 ata/0
  183 root       22   0     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_0
```

图 204 在诊断控制台中显示 CC-SG 进程

3. 键入 **h** 调出 top 命令详细帮助屏幕。标准的 **F1** 帮助键在此处不起作用。要返回管理员控制台，键入 **CTL+Q** 或 **CTL+C**。

显示网络时间协议 (NTP) 状态（实用工具）

如果在 CC-SG 上配置并运行 NTP，此选项显示 NTP 时间后台的状态。

要显示 CC-SG 上 NTP 后台的状态：

1. 单击“操作”、“实用工具”，然后单击“NTP 状态显示”。
2. NTP 后台只能在 CC-SG 管理员的 Director Client 上配置。如果 NTP 未启用或正确配置，则会显示以下内容：

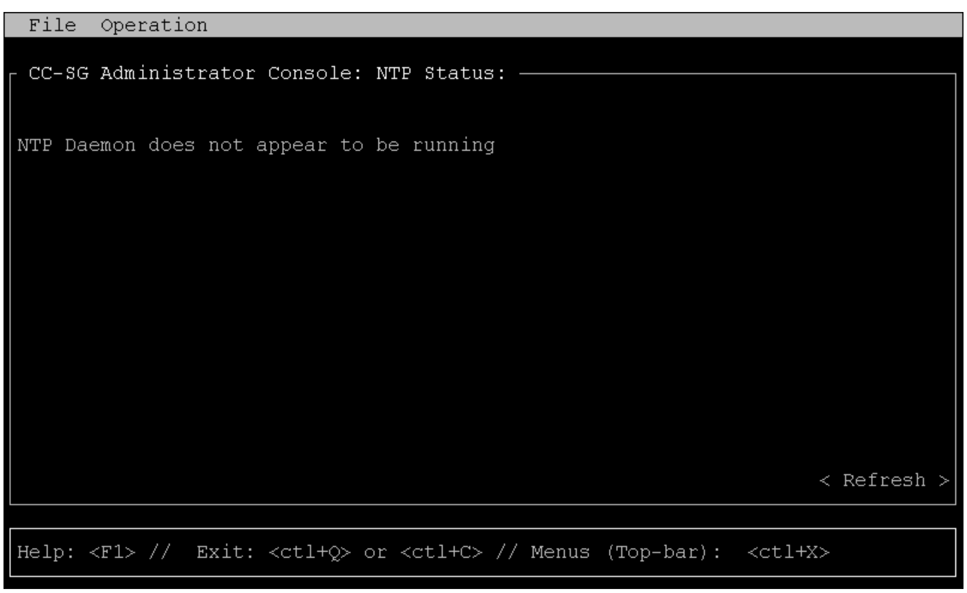


图 205 CC-SG GUI 中未配置 NTP

3. 如果在 CC-SG 上正确配置并正在运行 NTP，则会生成类似以下内容的显示：

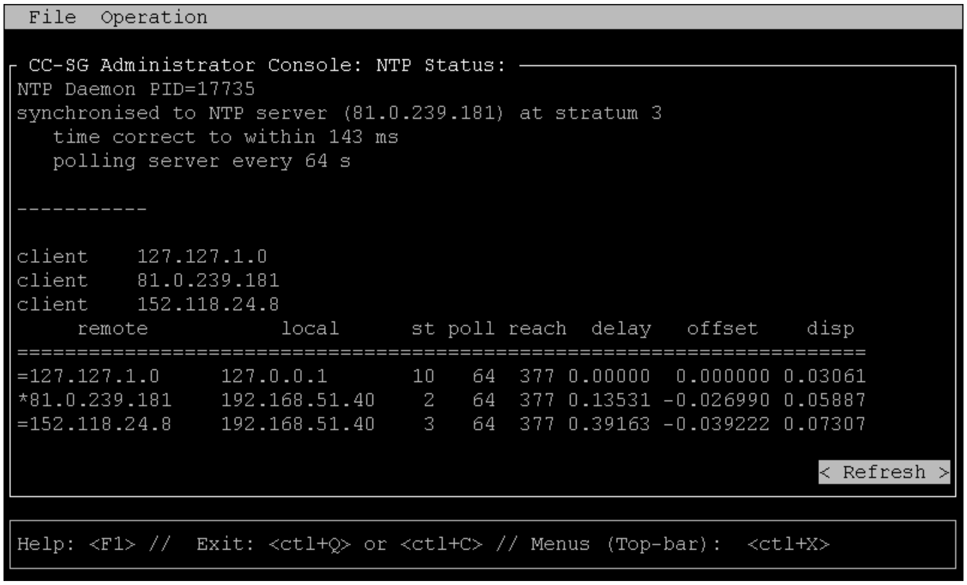


图 206 CC-SG GUI 中运行 NTP

4. 选择“刷新”将更新此页上的信息。

附录 A：规格（G1、V1 和 E1）

G1 平台

总体规格

形状因素	1U
尺寸 **(DxWxH)**	22.1”x 17.32” x 1.75” 563mm x 440mm x 44mm
重量	24.07 磅（10.92 公斤）
电源	冗余、可热插拔电源，自动检测 110/220 V – 2.0A
平均故障间隔时间 **(MTBF)**	38269 小时
KVM 管理端口	（DB15 + PS2 键盘/鼠标）
串行管理端口	DB9
控制台端口	不适用

硬件规格

处理器	Intel® Pentium® III 1 GHz
内存	512 MB
网络接口	(2) 10/100 以太网 (RJ45)
硬盘和控制器	(2) 40-GB IDE @7200 rpm, RAID 1
CD/ROM 驱动器	CD/ROM 40x 只读

环境要求

运行	
湿度	20% - 85% RH
海拔高度	海拔高度为 0 至 10000 英尺（3048 米）工作正常，存储 40000 英尺（12192 米）（估计）
振动	5-55-5 HZ，0.38mm，每个循环为 1 分钟；每个轴方向（X、Y、Z）各 30 分钟
冲击	不适用
非运行	
温度	0 - 30°C；32 – 104°F
湿度	10% - 90% RH
海拔高度	海拔高度为 0 至 10000 英尺（3048 米）工作正常，存储 40000 英尺（12192 米）（估计）
振动	5-55-5 HZ，0.38mm，每个循环为 1 分钟；每个轴方向（X、Y、Z）各 30 分钟
冲击	不适用

V1 平台

总体规格

形状因素	1U
尺寸 **(DxWxH)**	24.21"x 19.09" x 1.75" 615mm x 485mm x 44mm
重量	23.80 磅（10.80 公斤）
电源	单电源（1 x 300 瓦）
工作温度	10℃- 35℃ (50℉- 95℉)
平均故障间隔时间 **(MTBF)**	36354 小时
KVM 管理端口	（DB15 + PS2 或 USB 键盘/鼠标）
串行管理端口	DB9
控制台端口	2 个 USB 2.0 端口

硬件规格

处理器	AMD Opteron 146
内存	2 GB
网络接口	2 个 10/100/1000 以太网 (RJ45)
硬盘和控制器	2 个 80-GB SATA @ 7200 rpm, RAID 1
CD/ROM 驱动器	DVD-ROM

环境要求

运行	
湿度	8% - 90% RH
海拔高度	海拔高度为 0 至 10000 英尺（3048 米）工作正常，存储 40000 英尺（12192 米）（估计）
振动	5-55-5 HZ，0.38mm，每个周期为 1 分钟；每个轴方向（X、Y、Z）各 30 分钟
冲击	不适用
非运行	
温度	-40℃ - +60℃ (-40℉-140℉)
湿度	5% - 95% RH
海拔高度	海拔高度为 0 至 10000 英尺（3048 米）工作正常，存储 40000 英尺（12192 米）（估计）
振动	5-55-5 HZ，0.38mm，每个周期为 1 分钟；每个轴方向（X、Y、Z）各 30 分钟
冲击	不适用

E1 平台

总体规格

形状因素	2U
尺寸 **(DxWxH)**	27.05"x 18.7" x 3.46"—687 mm x 475 mm x 88 mm
重量	44.09 磅（20 公斤）
电源	SP502-2S 可热插拔 500W 2U 电源
工作温度	0~50℃
平均故障间隔时间 **(MTBF)**	53564 小时
KVM 管理端口	PS/2 键盘和鼠标端口，1 个 VGA 端口
串行管理端口	快速 UART 16550 串口
控制台端口	2 个 USB 2.0 端口

硬件规格

处理器	2 个 AMD Opteron 250 2.4G 1MB 处理器
内存	4 GB
网络接口	Intel PRO/1000 PT 双口服务器适配器
硬盘和控制器	(2) WD740ADFD SATA 74GB 10K RPM 16MB 高速缓存
CD/ROM 驱动器	DVD-ROM

环境要求

运行	
湿度	5-90%，无凝结
海拔高度	海平面至 7000 英尺（2133 米）
振动	每个垂直轴 X、Y 和 Z 上 10 Hz 至 500 Hz 扫频，0.5 g 等加速度，持续一个小时
冲击	每个垂直轴 X、Y 和 Z 上 5 g，持续 11 ms，使用 ½ 正弦波
非运行	
温度	-40-70℃
湿度	5-90%，无凝结
海拔高度	海平面至 40000 英尺（12192 米）
振动	每个垂直轴 X、Y 和 Z 上 10 Hz 至 300 Hz 扫频，2 g 等加速度，持续一个小时
冲击	每个垂直轴 X、Y 和 Z 上 30 g，持续 11 ms，使用 ½ 正弦波

此页专门留白。

附录 B：CC-SG 和网络配置

简介

本附录介绍典型 CC-SG 部署的网络要求（地址、协议和端口）。对于外部访问（如果需要）和内部安全性以及路由策略增强（如果使用），均提供了需要了解和网络配置的内容。对于 TCP/IP 网络管理员，其角色和职责可能超过 CC-SG 管理员，可能希望将 CC-SG 及其组件纳入现场的安全访问和路由策略，此处提供相关详细信息以方便其工作。

如下图所示，典型的 CC-SG 部署可能没有或拥有部分或全部功能，例如防火墙或虚拟专用网 (VPN)。后面的表格介绍了 CC-SG 及其相关组件所需的协议和端口，尤其在网络中存在防火墙或 VPN，且网络中要强制实施访问和安全策略时，这些一定要了解。

执行综合

在下面的小节中对 CC-SG 及其关联组件的通信和端口使用提供了完整而详尽的分析。有些客户仅想要知道在防火墙上要打开哪些端口以允许访问 CC-SG 及其控制的目标，则应打开以下端口：

端口号	协议	用途
80	TCP	至 CC-SG 的 HTTP 访问
443	TCP	至 CC-SG 的 HTTPS (SSL) 访问
8080	TCP	CC-SG <-> PC 客户端
2400	TCP	节点访问（代理模式和带内访问）
5000[1]	TCP	节点访问（直接模式）
51000[1]	TCP	SX 目标访问（直接模式）

此清单可进一步削减：

- 如果到 CC-SG 的所有访问都通过 HTTPS 地址，则端口 80 可关闭。
- 如果任何来自防火墙的连接都使用 CC-SG 代理模式，则端口 5000 和 51000 可关闭。

因此，最低配置仅需要打开三个端口（443、8080 和 2400）即可允许到 CC-SG 的外部访问。

在下面的小节中提供有关这些访问方法和端口的详细信息以及配置控制和选项。

[1] 需要按照将被外部访问的 Raritan 设备打开这些端口。表中的其它端口只有访问 CC-SG 时才需要打开。

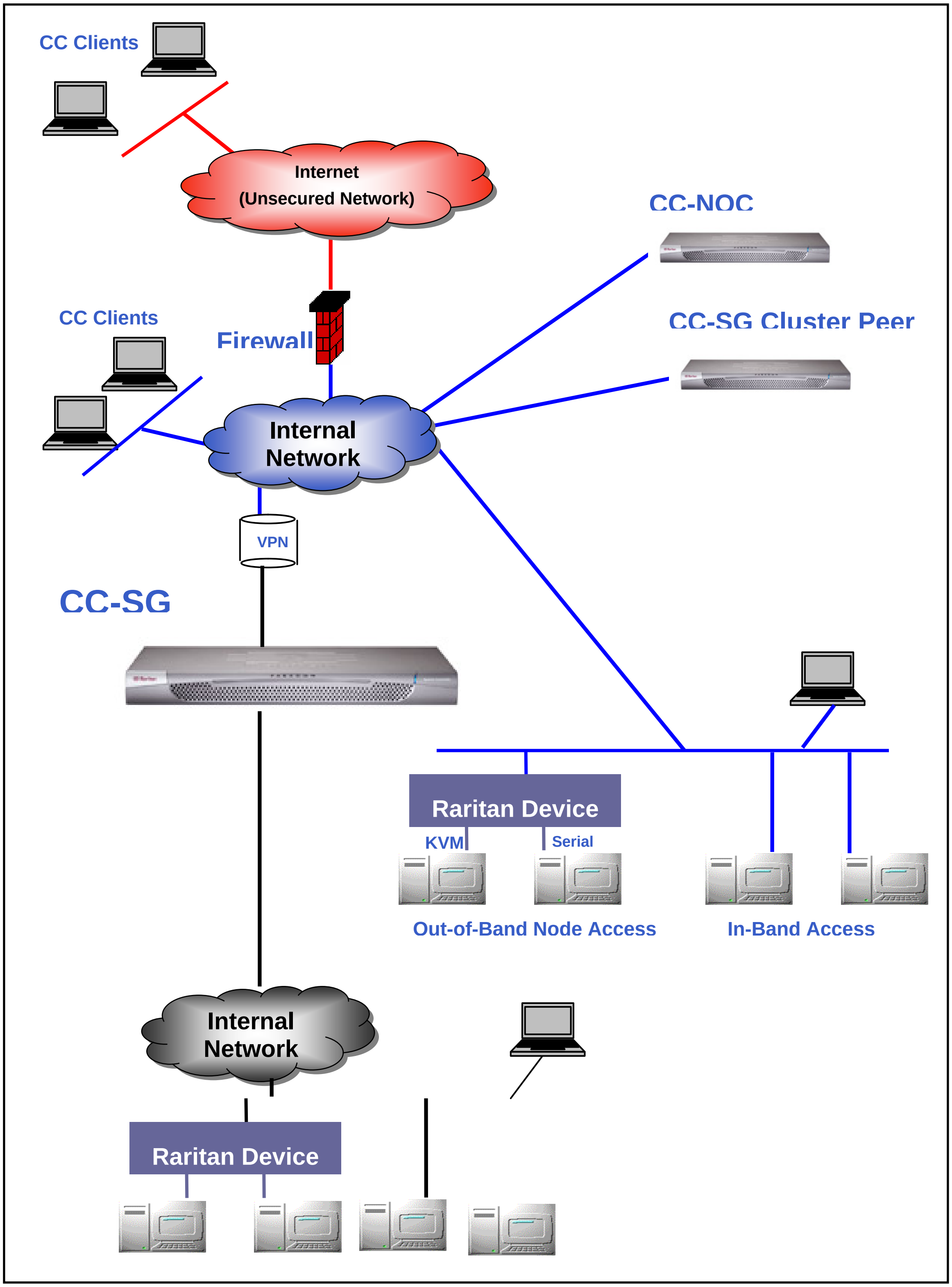


图 207 CC-SG 部署元素

CC-SG 通信通道

通信通道划分如下：

- CC-SG ↔ Raritan 设备
- CC-SG ↔ CC-SG 群集（可选）
- CC-SG ↔ 基础设施服务
- 客户端 ↔ CC-SG
- 客户端 ↔ 目标（直接模式）
- 客户端 ↔ 目标（代理模式）
- 客户端 ↔ 目标（带内）
- CC-SG ↔ CC-NOC

对于每个通信通道，后面的表格：

- 介绍通信方使用的象征性 **IP 地址**。在实体之间的所有通信通道上都要允许这些地址。
- 指出通信发起的**方向**。这对于特殊的站点策略可能非常重要。对于给定的 CC-SG 角色，相应通信方之间的路径必须可用，并用于出现网络中断时可能使用的代用重新路由路径。
- 提供 CC-SG 使用的**端口号**和**协议**。
- 指出端口是否**可配置**，这意味着 GUI 或诊断控制台提供字段用来将端口号从列出默认值改为其它值（因为与网络中的其它应用程序冲突，或为了安全原因）。

CC-SG 和 Raritan 设备

CC-SG 的主要角色是管理和控制 Raritan 设备（例如 Dominion KX、KSX 等）。通常，CC-SG 通过 TCP/IP 网络（局域网、广域网或 VPN）与这些设备通信，TCP 和 UDP 协议的使用如下：

通信方向	端口号	协议	可配置？
CC-SG → 本地广播	5000	UDP	是
CC-SG → 远程 LAN IP	5000	UDP	是
CC-SG → Raritan 设备	5000	TCP	是
Raritan 设备 → CC-SG	5001	UDP	否

CC-SG 群集

使用可选的 CC-SG 群集功能时（即两台 CC-SG 互联作为一台设备工作），以下端口必须提供为互联子网。（如果不使用可选的群集功能，则网络中不需要开放这些端口。）

群集中的每个 CC-SG 可能在单独的 LAN 上。但是，设备之间的互联应非常可靠，不容易发生拥塞。

通信方向	端口号	协议	可配置?
CC-SG → 本地广播	10000	UDP	否
CC-SG → 远程 LAN IP	10000	UDP	否
CC-SG ↔ CC-SG	5432	TCP	否
CC-SG ↔ CC-SG	8732	TCP	否
CC-SG ↔ CC-SG	3232	TCP	否

访问基础设施服务

CC-SG 可配置使用多种行业标准服务，例如 DHCP、DNS 和 NTP。为了能让 CC-SG 与这些可选的服务器通信，使用以下端口和协议：

通信方向	端口号	协议	可配置?
DHCP 服务器 → CC-SG	68	UDP	否
CC-SG → DHCP 服务器	67	UDP	否
NTP 时间服务器 ↔ CC-SG	123	UDP	否
CC-SG → DNS	53	UDP	否

PC 客户端至 CC-SG

PC 客户端通过以下模式连接 CC-SG：

- Web / Java Applet CC-SG GUI 接口
- 通过 SSH 的 CC-SG 命令行接口
- CC-SG 诊断控制台

第一种模式是用户和管理员连接 CC-SG 的主要方式。另外两种模式较为少用。这些模式需要以下网络配置：

通信方向	端口号	协议	可配置?
客户端 → CC-SG GUI	443	TCP	否
客户端 → CC-SG GUI	80	TCP	否
客户端 → CC-SG GUI	8080	TCP	否
客户端 → CC-CLI SSH	22	TCP	是
客户端 → CC 诊断控制台	23	TCP	是

PC 客户端至节点

CC-SG 另一种重要角色是将 PC 客户端连接到各种目标（或节点）。这些目标可以是到 Raritan 设备的串行或 KVM 控制台连接（叫做带外连接）。另一种模式是使用带内访问 (IBA) 方法，例如虚拟网络计算机 (VNC)、Windows 远程桌面 (RDP) 或 Secure Shell (SSH)。

PC 到目标通信的另一方面是：

- PC 客户端直接连接到目标（通过 Raritan 设备或带内访问），叫做**直接模式**。
- 或者，PC 客户端通过 CC-SG（充当应用程序防火墙）连接到目标，叫做**代理模式**。

通信方向	端口号	协议	可配置?
客户端 → CC-SG（通过代理）→ 目标	2400 （在 CC-SG 上）	TCP	否
客户端 → Raritan 目标（直接模式）	5000（设备上）	TCP	是
客户端 → Dominion SX →（直接模式）	51000	TCP	是

CC-SG 与 IPMI、iLO/RILOE、DRAC、RSA 的客户端

CC-SG 的另一个重要角色是管理第三方设备，例如 iLO/RILOE、惠普的 Integrated Lights Out/Remote Insight Lights Out 服务器等。iLO/RILOE 设备目标可直接打开或关闭或重新启动。智能平台管理接口 (IPMI) 服务器也可由 CC-SG 进行控制。Dell DRAC 和 RSA 目标也可由 CC-SG 进行管理。

通信方向	端口号	协议	可配置?
CC-SG → IPMI	623	UDP	否
CC-SG → iLO/RILOE（使用 HTTP 端口）	80 或 443	UDP	否
CC-SG → DRAC	80 或 443	UDP	否
CC-SG → RSA	80 或 443	UDP	否

CC-SG 和 SNMP

简单网络管理协议 (SNMP) 允许 CC-SG 向网络上的现有 SNMP 管理器推送 SNMP 陷阱（事件通知）。CC-SG 还支持与第三方企业管理解决方案（如 HP OpenView）的 SNMP GET/SET 操作。

通信方向	端口号	协议	可配置?
SNMP 管理器 → CC-SG	161	UDP	是
CC-SG → SNMP 管理器	162	UDP	是

CC-SG 和 CC-NOC

CC-NOC 是可与 CC-SG 联合部署的可选设备。CC-NOC 是一种网络监视设备，用于审计和监视 CC-SG 所管理的服务器、设备和 Raritan 设备的状态。

通信方向	端口号	协议	可配置?
CC-SG ↔ CC-NOC	9443	TCP	否

CC-SG 内部端口

CC-SG 使用几个端口用于内部功能，其本地防火墙功能阻止对这些端口的访问。但是，有些外部扫描器可能将这些检测为“被阻止”或“被过滤”。不需要对这些端口的外部访问，可以将其进一步阻止。当前使用的端口为：

1088、1098、2222、4444、4445、8009、8083 和 8093

除这些端口之外，CC-SG 还可能在 32xxx（或以上）范围内打开十几个 TCP 和 UDP 端口。不需要对这些端口的外部访问，可以阻止这些访问。

通过启用 NAT 防火墙的 CC-SG 访问

如果防火墙使用使用 NAT（网络地址转换）并可能使用端口地址转换 (PAT)，则使用此防火墙的所有连接都应使用代理模式。而且，防火墙上必须配置外部连接到端口 80（非 SSL）/443 (SSL)[2]、8080 和 2400 转发到 CC-SG（因为 PC 客户端将在这些端口上发起会话）。

所有带内访问 (IBA) 连接使用 CC-SG 作为代理连接，不需要其它配置。使用防火墙的带外访问 (OBA) 连接必须配置使用代理模式（“设置”➔“配置管理器”➔“连接模式”菜单）。这样，CC-SG 将代表 PC 客户端请求连接到各种目标（IBA 或 OBA）。但是，CC-SG 将终止通过防火墙的 PC 客户端到目标 TCP/IP 连接。

[2] 建议不要通过防火墙运行非 SSL 流量。

安全性和开放端口扫描

作为 CC-SG 质量保证过程的一部分，产品中应用几个开放端口扫描器，Raritan 保证其产品不易受到对这些已知攻击。所有开放的或过滤/阻止的端口都在上面各节内列出。以下为一些较为常见的暴露：

问题 ID[3]	概要	备注
CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516	snmp (161/UDP) - 远程 SNMP 服务器的公用串名称可以猜出。	默认的 CC-SG SNMP 公用串为“public”。鼓励用户将其更改为站点特定的值（“设置➔配置管理器➔SNMP”菜单）。详情参见《CC-SG 管理员指南》。
CVE-2000-0843	提供长用户名后跟密码时，远程 telnet 服务器突然关闭连接。	传统上，端口 23 用于 telnet 服务。但是 CC-SG 将此端口用于 SSH V2 诊断控制台会话。用户可更改此端口和/或完全禁用诊断控制台使用 SSH 访问方法。详情参见《CC-SG 管理员指南》。
CVE-2004-0230	远程主机容易受到序号近似缺陷的影响，可能会允许攻击者向远程主机发送欺骗 RST 包并关闭建立的连接。	CC-SG 使用的基础 TCP/IP 协议栈尚未显示为易受此暴露的影响。
CVE-2004-0079 CVE-2004-0081 CVE-2004-0112	远程主机使用的 OpenSSL 版本早于 0.9.6m 或 0.9.7d。	OpenSSL 已经应用以下补丁，因此可删除此暴露： • RHSA-2004:120 • RHSA-2005:830. • RHSA-2003:101-01

[3] CVE 可在以下位置查询 **http://cve.mitre.org**

此页专门留白。

附录 C：用户组权限

菜单 > 子菜单	菜单项	需要的权限	说明
Secure Gateway	**此菜单为所有用户可用。**		
	我的配置文件	无*	
	当日消息	无*	
	打印	无*	
	注销	无*	
	退出	无*	
用户	**此菜单和用户树仅可用于拥有“用户管理”权限的用户。**		
> 用户管理器	> 添加用户	用户管理	
	（编辑用户）	用户管理	通过用户配置文件
	> 删除用户	用户管理	
	> 从组中删除用户	用户管理	
	> 注销用户	用户管理	
	> 批量复制	用户管理	
> 用户组管理器	> 添加用户组	用户管理	
	（编辑用户组）	用户管理	通过用户组配置文件
	> 删除用户组	用户管理	
	> 将用户分配到组	用户管理	
	> 注销用户	用户管理	
设备	**此菜单和设备树仅可用于拥有以下任一权限的用户：** **设备、端口和节点管理** **设备配置和升级管理**		
	发现设备	设备、端口和节点管理	
> 设备管理器	> 添加设备	设备、端口和节点管理	
	（编辑设备）	设备、端口和节点管理	通过设备配置文件
	> 删除设备	设备、端口和节点管理	
	> 批量复制	设备、端口和节点管理	
	> 升级设备	设备配置和升级管理	
>> 配置	>> 备份	设备配置和升级管理	
	>> 恢复	设备配置和升级管理	
	>> 复制配置	设备配置和升级管理	
	> 重启设备	设备、端口和节点管理，或者设备配置和升级管理	
	> Ping 设备	设备、端口和节点管理，或者设备配置和升级管理	
	> 暂停管理	设备、端口和节点管理，或者设备配置和升级管理	

菜单 > 子菜单	菜单项	需要的权限	说明
	> 设备电源管理器	设备、端口和节点管理	
	> 启动管理	设备、端口和节点管理，或者设备配置和升级管理	
	> 启动用户工作站管理		
	> 断开用户连接	设备、端口和节点管理，或者设备配置和升级管理	
	> 拓扑视图	设备、端口和节点管理	
> 更改视图	> 创建自定义视图	设备、端口和节点管理，或者设备配置和升级管理	
	> 树形视图	设备、端口和节点管理，或者设备配置和升级管理	
> 端口管理器	> 连接	设备、端口和节点管理	
	> 配置端口	设备、端口和节点管理	
	> 书签端口	设备、端口和节点管理	
	> 断开端口连接	设备、端口和节点管理	
	> 批量复制	设备、端口和节点管理	
	> 删除端口	设备、端口和节点管理	
> 端口排序选项	> 按端口名称	设备、端口和节点管理，或者设备配置和升级管理	
	> 按端口状态	设备、端口和节点管理，或者设备配置和升级管理	
节点	**此菜单和节点树仅可用于拥有以下任一权限的用户：** **设备、端口和节点管理** **节点带内访问** **节点带外访问** **节点电源控制**		
	添加节点	设备、端口和节点管理	
	（编辑节点）	设备、端口和节点管理	通过节点配置文件
	删除节点	设备、端口和节点管理	
	<接口名称>	带内访问或 带外访问	
	断开连接	带内访问或 带外访问	
	电源控制	电源控制	
	组电源控制	电源控制	
> 节点排序选项	> 按节点名称	以下任一： 设备、端口和节点管理，或 带内访问或	

菜单 > 子菜单	菜单项	需要的权限	说明
		带外访问，或 电源控制	
	> 按节点状态	以下任一： 设备、端口和节点管理，或 节点带内访问或 节点带外访问，或 节点电源控制	
> 聊天	> 开始聊天	节点带内访问或 节点带外访问，或 节点电源控制	
	> 显示聊天会话	节点带内访问或 节点带外访问，或 节点电源控制	
	> 结束聊天会话	节点带内访问或 节点带外访问，或 节点电源控制	
> 更改视图	> 创建自定义视图	以下任一： 设备、端口和节点管理，或 节点带内访问或 节点带外访问，或 节点电源控制	
	> 树形视图	以下任一： 设备、端口和节点管理，或 节点带内访问或 节点带外访问，或 节点电源控制	
关联	**此菜单仅可用于拥有“用户安全管理”权限的用户。**		
	> 关联	用户安全管理	包括能够添加、修改和删除
	> 设备组	用户安全管理	包括能够添加、修改和删除
	> 节点组	用户安全管理	包括能够添加、修改和删除
	> 策略	用户安全管理	包括能够添加、修改和删除
报告	**此菜单为所有用户可用。**		
	审计跟踪	CC 设置和控制	

菜单 > 子菜单	菜单项	需要的权限	说明
	错误日志	CC 设置和控制	
	访问报告	仅为“系统管理员”组内的用户可用。	
	可用性报告	设备、端口和节点管理，或者设备配置和升级管理	
> 用户	> 活动用户	用户管理	
	> 锁定用户	CC 设置和控制	
	> 用户数据	要查看所有用户数据：用户管理 要查看自己的用户数据：无	
	> 组中的用户	用户管理	
	> 组数据	用户安全管理	
	> AD 用户组报告	CC 设置和控制，或用户管理	
> 设备	资产管理	设备、端口和节点管理	
> 节点	> 节点资产报告	设备、端口和节点管理	
	> 活动节点	设备、端口和节点管理	
	> 节点创建	设备、端口和节点管理	
> 端口	> 查询端口	设备、端口和节点管理	
	> 活动端口	设备、端口和节点管理	
	计划报告	CC 设置和控制	
	CC-NOC 同步	CC 设置和控制	
访问			
	CC-NOC 配置	CC 设置和控制	
管理	**此菜单仅可用于拥有以下任一权限的用户。** **CC 设置和控制** **设备、端口和节点管理以及用户安全管理的组合**		
	指导设置	以下全部： 设备、端口和节点管理以及用户安全管理	
	当日消息设置	CC 设置和控制	
	应用程序	CC 设置和控制	
	固件	CC 设置和控制	
	配置	CC 设置和控制	
	安全	CC 设置和控制	
	通知	CC 设置和控制	
	任务	CC 设置和控制	
	兼容性矩阵	设备配置和升级管理	

菜单 > 子菜单	菜单项	需要的权限	说明
系统维护			
	备份	CC 设置和控制	
	恢复	CC 设置和控制	
	复位	CC 设置和控制	
	重新启动	CC 设置和控制	
	升级	CC 设置和控制	
	关机	CC 设置和控制	
> 维护模式	> 进入维护模式	CC 设置和控制	
	> 退出维护模式	CC 设置和控制	
查看		无*	
窗口		无*	
帮助		无*	

*“无”表示不需要特殊的权限。任何可以访问 CC-SG 的用户都能够查看和访问这些菜单和命令。

此页专门留白。

附录 D：SNMP 陷阱

CC-SG 提供以下陷阱：

SNMP 陷阱	说明
ccUnavailable	CC-SG 应用程序不可用
ccAvailable	CC-SG 应用程序可用
ccUserLogin	CC-SG 用户登录
ccUserLogout	CC-SG 用户注销
ccPortConnectionStarted	CC-SG 会话启动
ccPortConnectionStopped	CC-SG 会话停止
ccPortConnectionTerminated	CC-SG 会话终止
ccImageUpgradeStarted	CC-SG 映像升级启动
ccImageUpgradeResults	CC-SG 映像升级结果
ccUserAdded	新用户添加到 CC-SG
ccUserDeleted	用户从 CC-SG 中删除
ccUserModified	CC-SG 用户已被修改
ccUserAuthenticationFailure	CC-SG 用户认证失败
ccLanCardFailure	C-SG 探测到 LAN 卡失效
ccHardDiskFailure	CC-SG 探测到硬盘失效
ccLeafNodeUnavailable	CC-SG 探测到至叶子节点的连接失败
ccLeafNodeAvailable	CC-SG 探测到叶子节点不可达
ccIncompatibleDeviceFirmware	CC-SG 删除含有不兼容固件的设备
ccDeviceUpgrade	CC-SG 已升级设备上的固件
ccEnterMaintenanceMode	CC-SG 进入维护模式
ccExitMaintenanceMode	CC-SG 退出维护模式
ccUserLockedOut	CC-SG 用户已被锁定
ccDeviceAddedAfterCCNOCNotification	从 CC-SG 接收到通知后，CC-NOC 已经添加了设备
ccScheduledTaskExecutionFailure	执行计划任务失败的原因
ccDiagnosticConsoleLogin	用户已经登录 CC-SG 诊断控制台
ccDiagnosticConsoleLogout	用户已从 CC-SG 诊断控制台注销
ccNOCAvailable	CC-SG 探测到 CC-NOC 可用
ccNOCUnavailable	CC-SG 探测到 CC-NOC 不可用
ccUserGroupAdded	新用户组已经添加到 CC-SG
ccUserGroupDeleted	CC-SG 用户组已被删除
ccUserGroupModified	CC-SG 用户组已被修改
ccSuperuserNameChanged	CC-SG 超级用户名称已更改
ccSuperuserPasswordChanged	CC-SG 超级用户密码已更改
ccLoginBannerChanged	CC-SG 登录条幅已更改
ccMOTDChanged	CC-SG 当日消息 (MOTD) 已更改

此页专门留白。

附录 E：故障排除

- 要从 Web 浏览器启动 CC-SG，需要一个 Java 插件。如果机器上的版本不正确，则 CC-SG 将引导完成安装步骤。如果机器上没有 Java 插件，CC-SG 无法自动启动。在这种情况下，必须卸载或禁用旧的 Java 版本，提供一个到 CC-SG 的串口连接才能正常操作。
- 如果 CC-SG Applet 不加载，请检查 Web 浏览器设置。
  - 在 Internet Explorer 中：确保启用 Java（Sun）。
  - 在“控制面板”中打开“Java 插件”，调节浏览器的设置。
- 如果添加设备遇到问题，确保设备具有正确的固件版本。
- 如果设备与 CC-SG 之间的网络接口电缆断开，等待配置的检测信号时间（分钟），然后插回网络接口电缆。在配置的检测信号周期内，设备以单机模式运行，可通过 RRC、MPC 或 RC 访问。
- 如果收到错误消息显示客户端版本与服务器版本不一致，且行为不可预测，则应重新启动并清空浏览器的高速缓冲。

客户端浏览器要求

有关所支持的浏览器和平台完整列表，请参照 **http://www.raritan.com/support** 上的“兼容性矩阵”。在“支持”页面上，单击“固件升级”，然后单击 **CommandCenter Secure Gateway**。

此页专门留白。

附录 F：双因素认证

作为基于 CC-SG RADIUS 的远程认证的一部分，通过关联的 RSA 认证管理器可将 CC-SG 配置为指向支持双因素认证的 RSA RADIUS 服务器。CC-SG 充当 RADIUS 客户端，将用户认证请求发送给 RSA RADIUS 服务器。认证请求包括用户 ID、固定密码和动态令牌代码。

支持的环境

以下的 RSA 双因素认证组件一种可用于 CC-SG。

- Windows Server 2003 上的 RSA RADIUS Server 6.1
- Windows Server 2003 上的 RSA Authentication Manager 6.1
- RSA Secure ID SID700 硬件令牌。

较早的 RSA 产品版本也应能够用于 CC-SG，但未经过验证。

设置要求

有关 RSA RADIUS 服务器和 RSA 认证管理器的正确配置不在本指南的涵盖范围之内。详情查阅 RSA 文档。

但是要注意一定要完成以下过程：

1. 导入令牌
2. 创建一个 CC-SG 用户并为其指定一个令牌。
3. 生成用户密码。
4. 为 RADIUS 服务器创建一个代理主机。
5. 为 CC-SG 创建一个代理主机（类型：通信服务器）。
6. 创建一个 RADIUS CC-SG 客户端。

已知问题

RSA RADIUS 的 New PIN 模式需要一个挑战密码/PIN，将无法工作。相反，在这种方案中的所有用户都必须指定固定密码。

此页专门留白。

附录 G：常见问题解答

问题	答案
常规	
何谓 CC-SG？	CC-SG 是一种网络管理设备，用于聚集和集成通常在数据中心部署的、与 Raritan 支持 IP 产品连接的多台服务器和网络设备。
为何需要 CC-SG？	随着部署的数据中心服务器和设备越来越多，其管理潜在地变得复杂。CC-SG 允许系统管理员或经理从单个设备访问和管理所有服务器、设备和用户。
何谓 CommandCenter NOC？	CommandCenter NOC 是一种网络监视设备，用于审计和监视 CC-SG 提供访问的服务器、设备和 Raritan 设备的状态。
CC-SG 支持哪些 Raritan 产品？	CC-SG 支持所有的 Dominion 产品 - Raritan 的 KVM over IP 产品 - Dominion KX - Raritan 的安全控制台服务器产品 - Dominion SX - Raritan 的远程办公室管理产品 - Dominion KSX CC-SG 在使用可选的 IP 用户工作站时也支持 Paragon II。
CC-SG 如何与其它 Raritan 产品集成？	CC-SG 使用独有的专有搜索和发现技术，识别和连接具有已知网络地址的所选 Raritan 设备。CC-SG 一旦连接和配置后，连接在 CC-SG 上的设备是透明的，操作和管理极其简单。
PDA 能访问吗？	一般答案：“是”，只要 PDA 有启用 Java 的浏览器并支持 128 位（或在某些地方较低的强度）SSL 加密。详情可致电 Raritan 技术支持。在这方面尚未进行测试。
CC-SG 的状态是否受限于它所代理的设备的状态？	否。因为 CC-SG 软件驻留在专用服务器上，即使被 CC-SG 代理的设备已经关闭，您仍然能够访问 CC-SG。
CC-SG 软件更新版本推出时，能升级使用更新版本吗？	是。直接与授权 Raritan 销售代表或 Raritan, Inc. 联系。
可以将多少个节点和/或 Dominion 设备和/或 IP-Reach 设备连接到 CC-SG？	对可以连接的节点数和/或 Dominion 和/或 IP-Reach 设备数没有具体限制。但这个数字并不是无限的：主服务器上的处理器性能和内存量将决定实际上可以连接的端口数。
如果 Microsoft Internet Explorer 是首选的 Web 浏览器，是否可以优化其性能？	在访问控制台时要优化 Microsoft IE 性能，禁用“启用虚拟主机的 JIT 编译器”、“启用 Java 日志”和“启用 Java 控制台”选项。 从主菜单中，选择“工具”> “Internet 选项”>“高级”。向下滚动找到上面的项目，确保其没有选中。
如果无法向 CC-SG 添加控制台/串行端口，该怎么办？	假设控制台/串行设备是 Dominion，保证满足以下条件： - Dominion 设备是活动的。 - Dominion 设备尚未达到最大配置用户帐户数量。
Raritan 的 CC-SG 支持哪个版本的 Java？	对于服务器和客户端侧的最低 Java 要求，参见 http://www.raritan.com/support 上的“兼容性矩阵”。单击“固件升级”，然后单击“CommandCenter Secure Gateway”。

问题	答案
管理员将一个新节点添加到 CC-SG 并将其分配给我，我如何在节点树内看到它？	要更新树并看到最新分配的节点，单击工具栏上的“刷新”快捷按钮。记住，刷新 CC-SG 将关闭所有当前的控制台会话。
将来会如何支持 Windows 桌面？	通过在防火墙上配置正确的端口，可从防火墙外部访问 CC-SG。以下为标准端口： 80: 用于通过 Web 浏览器的 HTTP 访问 443: 用于通过 Web 浏览器的 HTTPS 访问 8080: 用于 CC-SG 服务器操作 2400: 用于代理模式连接 5001: 用于 IPR/DKSX/DKX/ P2-SC 事件通知 如果两个群集节点之间存在防火墙，应打开以下端口让群集正常工作： 8732: 用于群集节点检测信号 5432: 用于群集节点 DB 复制
大型系统设计原则有哪些？有哪些限制或假设？	Raritan 提供两种服务器扩展模型：数据中心模型和网络模型。 数据中心模型使用 Paragon 在单个数据中心内扩展到上千个系统。这是扩展单个位置的最有效、最经济的方式。也支持通过 IP-Reach 和 IP 用户工作站（UST-IP）的网络模型。 网络模型通过使用 TCP/IP 网络进行扩展，并通过 CC-SG 聚集访问，因此用户不需要知道访问设备的 IP 地址或拓扑。它也提供单点登录的便利。
认证	
可为 CC-SG 创建多少个用户帐户？	检查您的许可限制。对可为 CC-SG 创建的用户帐户个数没有指定的限制，但个数并不是无限的。主机服务器上的数据库大小、处理器性能和内存量将决定实际上可创建的用户帐户个数。
能否将特定节点访问分配给特定用户？	是的，如果您拥有管理员权限的话。管理员能够按用户分配特定的节点。
如果我们有超过 1000 个用户，该如何进行管理？您是否支持 Active Directory？	CC-SG 能与 Microsoft Active Directory、Sun iPlanet 或 Novell eDirectory 配合工作。如果认证服务器内已有某个用户帐户，则 CC-SG 支持使用 AD/TACACS+/RADIUS/LDAP 认证的远程认证。
使用目录服务和安全工具（例如 LDAP、AD、RADIUS 等）认证有哪些可用的选项？	CC-SG 允许本地认证和远程认证。 支持的远程认证服务器包括：AD、TACACS+、RADIUS 和 LDAP。
安全	
有时我尝试登录时，会收到消息说“登录名不正确”，但我确定输入正确的用户名和密码。为什么？	每次开始登录 CC-SG 时会发出会话特定的 ID。此 ID 有超时功能，因此如果在超时之前没有登录设备，则会话 ID 即开始无效。执行一次“Shift-重新加载”刷新 CC-SG 的页面。或者，您可关闭当前的浏览器，打开新

问题	答案
	的浏览器，然后重新登录。这样提供附加的安全功能，没有人可能重新调出 Web 高速缓冲中存储的信息来访问设备。
密码的安全性如何？	密码使用 MD5 进行加密，这是一种单向散列。这样提供附加的安全性，访问非授权用户访问密码列表。
有时我离开工作站一段时间后，单击 CC-SG 上的任何菜单时会收到“没有登录”消息。为什么？	CC-SG 对每个用户会话进行定时。如果在预先定义的时间内没有活动，则 CC-SG 注销用户。该时间周期的长度预设为 60 分钟，但可进行重新配置。建议用户完成会话后要退出 CC-SG。
由于 Raritan 没有到服务器的 root 访问，这会导致政府机构产生潜在问题。客户能否具有 root 访问，或者 Raritan 能否提供一种可审计性/财务明确度的方法？	一旦设备运出 Raritan, Inc.，无人拥有对服务器的根访问权。
SSL 是否同时是内部和外部功能（而不仅仅是 WAN，也是 LAN 的功能）？	二者都有。会话的加密不论来源，LAN 或 WAN。
CC-SG 是否支持 CRL 列表，即无效证书的 LDAP 列表？	不。
CC-SG 是否支持客户端证书请求？	不。
帐务	
“审计跟踪”报告中的事件时间似乎不正确。为什么？	日志事件时间的记录是根据客户端计算机上的时间设置。可调整计算机的时间和日期设置。
审计/日志功能能否跟踪谁打开或关闭电源插头？	直接关电不被记录，但通过 CC-SG 的电源控制可记录到审计日志中。

性能	
作为 CC-SG 管理员，我添加了 500 多个节点并将其全部分配给自己。现在登录 CC-SG 需要很长时间。	作为管理员，当您被分配了很多节点时，CC-SG 在记录过程中会下载所有节点的全部信息，这会使过程大大减慢。对于主要用于管理 CC-SG 配置/设置的管理员帐户，建议不要向其分配很多节点。
每个客户端的带宽使用量是多大？	通过 TCP/IP 对串行控制台的远程访问与一个 telnet 会话具有相同水平的网络活动量。但是，它被限制于控制台端口本身的 RS232 带宽，加上 SSL/TCP/IP 开销。 Raritan 远程客户端（RRC）控制到 KVM 控制台的远程访问。此应用程序提供了可调节的带宽，从 LAN 级别直到适合远程拨号用户的级别。
分组	
是否可以将一个给定的服务器放到多个组内？	是。因为一个用户可属于多个组，一个设备可属于多个组。 例如，NYC 中的 Sun 可以是组“Sun”的一部分："Ostype = Solaris"，同时也是组“New York”的一部分："location = NYC"
对于将通过控制台端口活动使用阻止的其它使用，什么会对其产生影响？比如有些 Unix 变量不允许对网络接口进行管理。	控制台通常被认为是最后一着以后的安全和可靠的访问路径。有些 UNIX 系统仅允许在控制台上进行根登录。出于安全原因，其它系统可能防止多次登录，这样如果管理员登录到控制台，则其它访问即被拒绝。最后从控制台上，管理员可在需要阻止所有其它访问时禁用网络接口。 控制台上的正常命令活动与任何其它接口上同样的命令相比，影响不会更大。但是，由于它不决定于网络，系统因过度超载而无法响应网络登录时，却仍支持控制台登录。因此，控制台访问的另外一个好处就是对系统和网络问题进行故障排除和诊断。
对于在物理级别被移动/更换的 CIM 且对逻辑数据库产生更改的问题，您将如何建议？	每个 CIM 包含一个序列号和目标系统名称。我们的系统假设在交换机之间移动连接时，CIM 仍保持联系其命名的目标。这种移动自动反映在系统配置中，并传播到 CC-SG 中。相反，如果 CIM 被移到另外一台服务器，管理员必须对其重新命名。
互通性	
CC-SG 如何与 Blade Chassis 产品集成？	CC-SG 可支持任何使用 KVM 或串口的设备作为透明穿通。
CC-SG 能够与第三方 KVM 工具的集成达到什么级别，直到第三方 KVM 端口级别或者只是设备级别？	第三方 KVM 交换机集成一般通过键盘宏来完成，如果第三方 KVM 供应商不公布第三方 KVM 交换机的通信协议。根据第三方 KVM 交换机的功能，集成的紧密程度可能不同。
如何通过任何 IP-Reach 设备移植四个同时路径的限制，包括潜在 8 路径设备的路线图？	目前，最可能的实现方法是将 IP-Reach 与 CC-SG 聚合。将来，Raritan 计划增加每个设备的同时访问路径个数。但是这些计划尚未完成开发阶段，因为其它项目较为优先，但我们欢迎有关市场需求和 8 路径解决方案使用案例的建议。
授权	

通过 RADIUS/TACACS/LDAP 能否实现授权？	LDAP 和 TACACS 仅用于远程认证而非授权。
用户体验	
关于通过网络端口或本地串口（例如 COM2）的控制台管理：日志记录会做哪些操作，CC-SG 是否捕获本地管理，这是否会丢失？	通过 CC-SG 本身登录 CC-SG 如同在运行 CC-SG 的操作系统（Linux）上获取根权限。Syslog 将记录此类事件，但 CC-SG 控制台本身的用户类型信息将会丢失。

此页专门留白。

附录 H：键盘快捷键

在 Director Client 中可使用以下键盘快捷键。

操作	键盘快捷键
刷新	F5
打印面板	Ctrl + P
帮助	F1
在“关联”表内插入行	Ctrl + I

北美总部

Raritan
400 Cottontail Lane
Somerset, NJ 08873
U.S.A.
电话 (732) 764-8886
或 (800) 724-8090
传真 (732) 764-8887
电子邮件：sales@raritan.com
网站：Raritan.com

Raritan NC
4901 Waters Edge Dr.
Suite 101
Raleigh, NC 27606
电话 (919) 277-0642
电子邮件：sales.nc@raritan.com
网站：Raritan.com

Raritan Canada
4 Robert Speck Pkwy, Suite 1500
Mississauga, ON L4Z 1S1 Canada
电话(905) 949-3650
传真 (905) 949-3651
电子邮件：sales.canada@raritan.com
网站：Raritan.ca

欧洲总部

Raritan Netherlands
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands（荷兰）
电话 (31) 10-284-4040
传真 (31) 10-284-4049
电子邮件：sales.europe@raritan.com
网站：Raritan.info

Raritan Germany
Lichtstraße 2
D-45127 Essen, Germany
电话 (49) 201-747-98-0
传真 (49) 201-747-98-50
电子邮件：
sales.germany@raritan.com
网站：Raritan.de

Raritan France
120 Rue Jean Jaurés
92300 Levallois-Perret, France
电话 (33) 14-756-2039
传真 (33) 14-756-2061
电子邮件：sales.france@raritan.com
网站：Raritan.fr

Raritan U.K.
36 Great St. Helen's
London EC3A 6AP,United Kingdom
电话 (44) 20-7614-7700
传真 (44) 20-7614-7701
电子邮件：sales.uk@raritan.com
网站：Raritan.co.uk

Raritan Italy
Via dei Piatti 4
20123 Milan, Italy
电话 (39) 02-454-76813
传真 (39) 02-861-749
电子邮件：sales.italy@raritan.com
网站：Raritan.it

日本总部

Raritan Japan
4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-Ku
Tokyo 104-0033, Japan
电话 (81) 03-3523-5991
传真 (81) 03-3523-5992
电子邮件：sales@raritan.co.jp
网站：Raritan.co.jp

Raritan Osaka
1-15-8 Nishihonmachi, Nishi-ku
Osaka 550-0005, Japan
电话 (81) (6) 4391-7752
传真 (81) (6) 4391-7761
电子邮件：sales@raritan.co.jp
网站：Raritan.co.jp

亚太总部

Raritan Taiwan
5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien City
Taipei Hsien, Taiwan, ROC
电话 (886) 2 8919-1333
传真 (886) 2 8919-1338
电子邮件：sales.taiwan@raritan.com
中文网站：Raritan.com.tw
英文网站：Raritan-ap.com

Raritan Shanghai
中国上海零陵路 899 号飞洲国际 17E 室
（邮编 200030）
电话 (86) 215425-2499
传真 (86) 215425-3992
电子邮件：sales.china@raritan.com
网站：Raritan.com.cn

Raritan Beijing
中国北京朝阳区霄云路 36 号国航大厦
1310 室（邮编 100027）
电话:(86) 10 8447-5706
传真 (86) 10 8447-5700
电子邮件：sales.china@raritan.com
网站：Raritan.com.cn

Raritan Guangzhou
中国广州天河北路 183 号大都会广场
1205/F（邮编 510075）
电话 (86-20) 8755 5581
传真 (86-20) 8755 5571
电子邮件：sales.china@raritan.com
网站：Raritan.com.cn

Raritan Korea
#3602, Trade Tower,
World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
电话 (82) 2 557-8730
传真 (82) 2 557-8733
电子邮件：sales.korea@raritan.com
网站：Raritan.co.kr

Raritan Australia
Level 2, 448 St Kilda Road,
Melbourne, VIC 3004, Australia
电话 (61) 3 9866-6887
传真 (61) 3 9866-7706
电子邮件：sales.au@raritan.com
网站：Raritan.co.au

Raritan India
210 2nd Floor Orchid Square Sushant Lok 1,
Block B, Gurgaon 122 002 Haryana
India
电话 (91) 124 5107881
传真 (91) 124 5107880
电子邮件：sales.india@raritan.com
网站：Raritan.co.in

Raritan OEM 部门

Peppercon AG, Raritan OEM Division
Scheringerstrasse 1
08056 Zwickau Germany
电话 (49) 375-27-13-49-0
电子邮件：info@peppercon.com
网站：www.peppercon.de